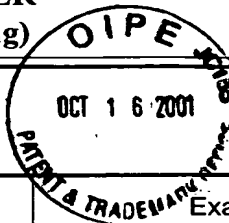


TRANSMITTAL LETTER
(General - Patent Pending)

Docket No.
112857-075

In Re Application Of: Haruo Oba et al.



Serial No.
09/696,927

Filing Date
October 26, 2000

Examiner

Group Art Unit

Title: AUTHENTICATION INFORMATION COMMUNICATION SYSTEM AND METHOD, PORTABLE
INFORMATION PROCESSING DEVICE AND PROGRAM FURNISHING MEDIUM

RECEIVED

OCT 19 2001

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Technology Center 2100

Transmitted herewith is:

Certified copy of Japanese Priority Document Numbers 11-310517 and 2000-253305

in the above identified application.

- ☒ No additional fee is required.
- ☐ A check in the amount of _____ is attached.
- ☒ The Assistant Commissioner is hereby authorized to charge and credit Deposit Account No. 02-1818 as described below. A duplicate copy of this sheet is enclosed.
- ☐ Charge the amount of _____
- ☐ Credit any overpayment.
- ☒ Charge any additional fee required.

Signature

William E. Vaughan (Reg. No. 39,056)
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690

Dated: October 9, 2001

I certify that this document and fee is being deposited
on October 9, 2001 with the U.S. Postal Service as
first class mail under 39 C.F.R. 111.3 and is addressed to the
Assistant Commissioner for Patents, Washington, D.C.
20231.

Signature of Person Mailing Correspondence

Robert Buccieri

Typed or Printed Name of Person Mailing Correspondence

CC:



日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

RECEIVED #8
OCT 19 2001
Technology Center 2100

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年11月 1日

出願番号

Application Number:

平成11年特許願第310517号

出願人

Applicant (s):

ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 9月18日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3073600

【書類名】 特許願

【整理番号】 99007026

【提出日】 平成11年11月 1日

【あて先】 特許庁長官殿

【国際特許分類】 G06K 17/00

【発明の名称】 認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体

【請求項の数】 24

【発明者】

 【住所又は居所】 東京都品川区東五反田3丁目14番13号 株式会社ソニーコンピュータサイエンス研究所内

 【氏名】 大場 晴夫

【発明者】

 【住所又は居所】 東京都品川区東五反田3丁目14番13号 株式会社ソニーコンピュータサイエンス研究所内

 【氏名】 戸塚 恵一

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社内

 【氏名】 沼岡 千里

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100101801

 【弁理士】

 【氏名又は名称】 山田 英治

 【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体

【特許請求の範囲】

【請求項 1】

人体を介した通信を行なう携帯情報処理装置とサービス提供装置とによって構成される認証情報通信システムにおいて、

前記携帯情報処理装置は、

人体と接触して人体を介した通信路を形成する接点 A と、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段とを有し、

前記サービス提供装置は、

人体と接触して人体を介した通信路を形成する接点 B と、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御手段と、

を有することを特徴とする認証情報通信システム。

【請求項 2】

前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、

該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを特徴とする請求項 1 に記載の認証情報通信システム。

【請求項 3】

前記サービス提供装置は、

前記携帯情報処理装置から、前記接点 A 及び接点 B を介して転送される前記認

証用データに基づく認証処理を実行する認証手段を有し、

前記制御手段は、該認証手段の認証処理結果に基づいてサービスの実行を制御する構成を有することを特徴とする請求項 1 に記載の認証情報通信システム。

【請求項 4】

前記サービス提供装置は、

提供するサービスに応じたサービス識別子を保持するサービス識別子保持手段を有し、

前記携帯情報処理装置は、

前記可変データ記憶手段に、前記サービス識別子に対応して前記可変ユーザ識別データを格納する構成を有し、

前記サービス提供装置から前記接点 B および前記接点 A を介して受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする請求項 1 に記載の認証情報通信システム。

【請求項 5】

前記サービス提供装置は、

提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、

前記携帯情報処理装置は、

前記認証用ユーザ識別データ生成手段の生成した認証用ユーザ識別データを前記サービス提供装置から前記接点 B、接点 A を介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする請求項 1 に記載の認証情報通信システム。

【請求項 6】

前記認証情報通信システムは、さらに、

ユーザに対する認証処理を実行するユーザ管理手段を有し、

前記ユーザ管理手段は、

ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを有し、該登録テーブルに基づいて認証処理を実行する構成を有すること

を特徴とする請求項 1 に記載の認証情報通信システム。

【請求項 7】

前記認証情報通信システムは、さらに、

ユーザに対する提供サービスを登録するサービス登録手段を有し、

該サービス登録手段は、

前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、

前記携帯情報処理装置は、

前記サービス登録手段において生成された認証用ユーザ識別データを前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする請求項 1 に記載の認証情報通信システム。

【請求項 8】

前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする請求項 1 に記載の認証情報通信システム。

【請求項 9】

サービス提供装置と人体を介して通信を実行する携帯情報処理装置において、人体と接触して人体を介した通信路を形成する接点 A と、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段と、

を有することを特徴とする携帯情報処理装置。

【請求項 10】

前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、

該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づ

く認証用データを生成する構成を有することを特徴とする請求項9に記載の携帯情報処理装置。

【請求項11】

前記携帯情報処理装置は、

前記可変データ記憶手段に、前記可変ユーザ識別データをサービス識別子に対応させて格納する構成を有し、

前記サービス提供装置から受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする請求項9に記載の携帯情報処理装置。

【請求項12】

前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする請求項9に記載の携帯情報処理装置。

【請求項13】

前記接点Aは、人体の装着部に沿った曲線形状を有することを特徴とする請求項9に記載の携帯情報処理装置。

【請求項14】

前記携帯情報処理装置は、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有することを特徴とする請求項9に記載の携帯情報処理装置。

【請求項15】

前記携帯情報処理装置は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレットのいずれかに内蔵された構成を有することを特徴とする請求項9に記載の携帯情報処理装置。

【請求項16】

前記固定データ記憶部と前記可変データ記憶部は前記携帯情報処理装置に対して着脱可能な構成を有することを特徴とする請求項9に記載の携帯情報処理装置。

【請求項17】

人体と接触して人体を介した通信路を形成する接点Aを有する携帯情報処理装

置と人体と接触して人体を介した通信路を形成する接点Bを有するサービス提供装置とによって実行される認証情報通信方法において、

前記サービス提供装置から前記携帯情報処理装置に対して、前記接点Bおよび接点Aを介してサービス識別データを転送するステップと、

前記携帯情報処理装置において、前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記携帯情報処理装置から前記サービス提供装置に対して、前記接点Aおよび接点Bを介して前記認証用データを出力するステップと、

前記サービス提供装置において、前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、
を有することを特徴とする認証情報通信方法。

【請求項 18】

前記認証用データ生成ステップは、

前記可変ユーザ識別データと、固定ユーザ識別データとを合成する合成ステップを含むことを特徴とする請求項 17 に記載の認証情報通信方法。

【請求項 19】

前記サービス提供装置は、

前記携帯情報処理装置から、前記接点A及び接点Bを介して転送される前記認証用データに基づく認証処理を実行する認証処理ステップを実行し、

前記制御ステップは、該認証処理ステップの認証処理結果に基づいてサービスの実行を制御することを特徴とする請求項 17 に記載の認証情報通信方法。

【請求項 20】

前記認証情報通信方法において、

前記サービス提供装置は、

さらに、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを有し、

前記携帯情報処理装置は、

前記認証用ユーザ識別データ生成ステップにおいて生成した認証用ユーザ識別データを前記サービス提供装置から前記接点B、接点Aを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納することを特徴とする請求項17に記載の認証情報通信方法。

【請求項21】

前記認証情報通信方法において、さらに、
ユーザに対する認証処理を実行するユーザ管理ステップを有し、
前記ユーザ管理ステップは、
ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを生成するステップを含み、
前記認証処理は、該登録テーブルに基づいて実行することを特徴とする請求項17に記載の認証情報通信方法。

【請求項22】

前記認証情報通信方法において、さらに、
ユーザに対する提供サービスを登録するサービス登録ステップを有し、
該サービス登録ステップは、
前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを含み、
前記携帯情報処理装置は、前記サービス登録ステップにおいて生成された認証用ユーザ識別データを可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納するステップを有することを特徴とする請求項17に記載の認証情報通信方法。

【請求項23】

人体と接触して人体を介した通信路を形成する接点Aを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Bを有するサービス提供装置とによって実行される認証情報通信システムにおいて、サービス提供装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記接点Bを介して前記携帯情報処理装置に対して、サービス識別データを出力するステップと、

前記サービス識別データに対応する可変ユーザ識別データに基づいて前記携帯情報処理装置が生成した認証用データを前記接点Bを介して受信するステップと

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とするプログラム提供媒体。

【請求項24】

人体と接触して人体を介した通信路を形成する接点Aを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Bを有するサービス提供装置とによって実行される認証情報通信システムにおいて、携帯情報処理装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記携帯情報処理装置に対して出力されるサービス識別データを前記接点Aを介して受信するステップと、

前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記サービス提供装置に対して、前記接点Aを介して前記認証用データを出力するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体に関する。さらに詳細には、外部機器に設けた電極である接点に人体の一部、例えば手が接触することによって、人体に装着したや

はり電極としての接点を設けた携帯機器とのデータ通信を可能とし、個人認証に必要なデータを人体を介して転送して個人認証処理、および外部機器との情報交換を可能にした個人認証情報通信システムおよび個人認証情報通信方法に関する構成を開示するものである。本発明に適用される携帯機器は、例えば時計や指輪のように曲線状の形状を有する取付具部を有し、人が通常身につける小型の物品において実現され、これらの装身具に個人認証のためのデータを記憶する構成としたものである。

【0002】

【従来の技術】

従来、非接触型カード等を利用して個人認証を行い、認証の可否に基づいて外部装置を制御するシステムは良く知られている（例えば特開平11-161763など）。非接触型カードは、定期券、プリペイドカード等の接触型カードに変わるシステムとして今後有効な手法として期待される構成の一つである。

【0003】

しかしながら、このような非接触型カードを使用するユーザは、カードによる認証を受ける場合、カード自体を手に取り、例えばセンサ等の情報読み取り装置に取りだしたカードを近づけて読み取り処理を実行させる必要があり、これらの各処理に時間を要するという欠点がある。例えば入場ゲート、改札を通過するときなどの限られた時間内に一連の処理を次々と実行させなければならない場合、個人認証のためのカード読み取り、読み取りデータに基づく認証処理、認証処理に基づく改札ゲートの開閉動作を複数のユーザに対して次々と実行する必要があり、1人あたりの処理時間の増加は多人数の処理においてさらに大きな処理時間の増加をもたらし、実用化を困難にする原因となっている。この意味で非接触型カードは従来の接触型カードに比較して、すべての面で優れているとは言い難い。

【0004】

さらに、非接触型カードまたはカード型以外の認証用携帯機器を使用するユーザは、ユーザが取り出した、または身につけたカード等の認証機器を認証装置あるいは処理装置に近づける、あるいは近くを通りすぎる等、きわめて曖昧な処理

を実行することが要求され、認証装置あるいは処理装置に直接触れるという処理を伴わないので、実際にデータの読み取りに成功しているのか、または個人認証処理が実行されているのか等の実感が得られず、処理の開始タイミング等が全くユーザには判別できない。従って、処理が遂行されているか否かの判定が曖昧になってしまい、結果として、所定時間後に例えばゲートが開かないといったエラーが生じ、このエラーが生じるまでは、読み取り処理の失敗、または認証されなかったという結果が得られないという欠点がある。

【 0 0 0 5 】

本発明の個人認証情報通信システムおよび個人認証情報通信方法は、係る状況に鑑み、従来の接触型カード、非接触型カードと同様に個人認証を実行して各種の処理を実行させるシステムおよび方法において、個人認証を行なおうとするユーザが認証システムを構成する装置に形成された接点に対して人体の一部、例えば指、または手のひら等を接触させることで人体を介して個人認証用データ転送を行ない、ユーザの個人認証処理の開始をユーザ自身が認識することを可能とし、個人認証処理システムの使い勝手を改善するとともに、ユーザに対して認証処理及び認証処理に基づく各種処理の実行が開始されたことの達成感を与えることができるシステムを提供するものである。

【 0 0 0 6 】

上述のような人体を介してデータ転送を行なうシステムを開示した従来例としては、例えば以下に示すものがある。

【 0 0 0 7 】

特開平 7 - 1 7 0 2 1 5、USP 5, 9 1 4, 7 0 1 には、電極を有する 2 つの互いに独立なシステムにおいて、そのままでは互いに通信するには不十分な程度の微弱電波をシステム間で発信し、そのシステム間に人体が介在することにより、人体を媒介としてシステム間のデータ転送を実行する構成が開示されている。例えば特開平 7 - 1 7 0 2 1 5 では、オーディオ／ビデオ信号等を導電性部材と人体を介して転送し、ディスプレイ、スピーカを備えた受信端末に出力する構成が記載されている。

【 0 0 0 8 】

また、USP 5, 796, 827では、人体を介したデータ転送を使用したシステムにおいて、さらに暗号化したデータを送受する手段を加えることによって、クレジットカードあるいはキャッシュカードなどに応用するというアイデアを開示している。具体的には、送信機から受信機に対する符号化データの転送を人体を伝送媒体として実行し、受信機に接続された認証処理装置が人体を介して送られた符号化データを処理して認証を行なう構成である。当USP 5, 796, 827では、人体を介するデータ転送を実行するための電極をユーザが日常、身につける物品に組み込み可能とした構成が示され、その例として腕時計、衣服、または靴が記載されている。このような日常的に体に接触している物品、いわゆる装身具に電極を組み込むことにより、ユーザが専用の電極構成体を新たに装着することを不要としている。

【0009】

【発明が解決しようとする課題】

しかしながら、昨今サービスの種類は多様化し、認証処理を行なった後に実行すべき処理の態様は、ユーザによっても、また場所、時間によっても異なるものとするのが好ましい場合が多い。ユーザを認証処理によって識別して一律に認証の可否に応じた処理を実行することは、提供されるサービスの内容が固定的になり好ましくない。例えば、情報提供サービスを実行するサービス提供端末において、BGM提供を受けようとする、ユーザAは、クラシックが好みであり、ユーザBはロックが好みである場合、単なる認証処理に基づいて、同一の音楽配信をすると好みと無関係な音楽情報が配信される。あるいはサービス提供端末が遊園地のゲートの開閉処理を制御する端末である場合、ユーザ毎にゲート開閉の有効時間、有効場所を設定することが望ましい。

【0010】

もちろん、ユーザ毎に提供サービスを設定するテーブルを設け、ユーザIDに基づいて提供サービスを決定し、決定したサービスを実行することも可能であるが、これらのデータ処理、すなわち情報提供端末からの中央処理装置へのデータ転送、データ処理装置におけるデータ処理、処理態様決定、さらに情報提供装置へのデータ転送等に時間を要し、次々に異なるユーザに対する処理を実行しなけ

ればならない環境等においては、処理時間の遅延が蓄積してしまうことになる。

【0011】

係る事情に鑑み、本発明は、ユーザ毎、サービス毎に異なる態様での処理を即座に実行可能にするように、各サービス毎に独立であり、かつ各ユーザ毎にユニークである認証用データを作成し、これをユーザの携帯機器に格納し、サービスの要求時にこの認証用データを出力できるようにしたものである。

【0012】

さらに本発明は、非接触型カードが持つ利便性を損なうことなく、ユーザがサービス提供端末の接点に触れることによってユーザに処理の達成感を与えることができるように、人体を介して通信を行う携帯情報処理装置の接点を人体に接触した状態で装着するため、曲線状の接点部を持つ構成としたものである。

【0013】

【課題を解決するための手段】

本発明は、上記課題を参酌してなされたものであり、その第1の側面は、人体を介した通信を行なう携帯情報処理装置とサービス提供装置とによって構成される認証情報通信システムにおいて、

前記携帯情報処理装置は、

人体と接触して人体を介した通信路を形成する接点Aと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段とを有し、

前記サービス提供装置は、

人体と接触して人体を介した通信路を形成する接点Bと、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御手段と、を有することを特徴とする認証情報通信システムにある。

【0014】

さらに、本発明の認証情報通信システムにおいて、前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを特徴とする。

【0015】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、前記携帯情報処理装置から、前記接点A及び接点Bを介して転送される前記認証用データに基づく認証処理を実行する認証手段を有し、前記制御手段は、該認証手段の認証処理結果に基づいてサービスの実行を制御する構成を有することを特徴とする。

【0016】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、提供するサービスに応じたサービス識別子を保持するサービス識別子保持手段を有し、前記携帯情報処理装置は、前記可変データ記憶手段に、前記サービス識別子に対応して前記可変ユーザ識別データを格納する構成を有し、前記サービス提供装置から前記接点Bおよび前記接点Aを介して受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする。

【0017】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、前記携帯情報処理装置は、前記認証用ユーザ識別データ生成手段の生成した認証用ユーザ識別データを前記サービス提供装置から前記接点B、接点Aを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする。

【0018】

さらに、本発明の認証情報通信システムは、さらに、ユーザに対する認証処理を実行するユーザ管理手段を有し、前記ユーザ管理手段は、ユーザ登録状況およ

び、登録ユーザごとのサービス利用状況を登録した登録テーブルを有し、該登録テーブルに基づいて認証処理を実行する構成を有することを特徴とする。

【0019】

さらに、本発明の認証情報通信システムは、さらに、ユーザに対する提供サービスを登録するサービス登録手段を有し、該サービス登録手段は、前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、前記携帯情報処理装置は、前記サービス登録手段において生成された認証用ユーザ識別データを前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする。

【0020】

さらに、本発明の認証情報通信システムにおいて、前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする。

【0021】

さらに、本発明の第2の側面は、
サービス提供装置と人体を介して通信を実行する携帯情報処理装置において、
人体と接触して人体を介した通信路を形成する接点Aと、
ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、
サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、
少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段と、

を有することを特徴とする携帯情報処理装置にある。

【0022】

さらに、本発明の携帯情報処理装置は、前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを

特徴とする。

【 0 0 2 3 】

さらに、本発明の携帯情報処理装置は、前記可変データ記憶手段に、前記可変ユーザ識別データをサービス識別子に対応させて格納する構成を有し、前記サービス提供装置から受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする。

【 0 0 2 4 】

さらに、本発明の携帯情報処理装置において、前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする。

【 0 0 2 5 】

さらに、本発明の携帯情報処理装置において、前記接点 A は、人体の装着部に沿った曲線形状を有することを特徴とする。

【 0 0 2 6 】

さらに、本発明の携帯情報処理装置は、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有することを特徴とする。

【 0 0 2 7 】

さらに、本発明の携帯情報処理装置は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレットのいずれかに内蔵された構成を有することを特徴とする。

【 0 0 2 8 】

さらに、本発明の携帯情報処理装置において、前記固定データ記憶部と前記可変データ記憶部は前記携帯情報処理装置に対して着脱可能な構成を有することを特徴とする。

【 0 0 2 9 】

さらに、本発明の第 3 の側面は、

人体と接触して人体を介した通信路を形成する接点 A を有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点 B を有するサービス提供装置とによって実行される認証情報通信方法において、

前記サービス提供装置から前記携帯情報処理装置に対して、前記接点 B および接点 A を介してサービス識別データを転送するステップと、

前記携帯情報処理装置において、前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記携帯情報処理装置から前記サービス提供装置に対して、前記接点 A および接点 B を介して前記認証用データを出力するステップと、

前記サービス提供装置において、前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とする認証情報通信方法にある。

【 0 0 3 0 】

さらに、本発明の認証情報通信方法において、前記認証用データ生成ステップは、前記可変ユーザ識別データと、固定ユーザ識別データとを合成する合成ステップを含むことを特徴とする。

【 0 0 3 1 】

さらに、本発明の認証情報通信方法において、前記サービス提供装置は、前記携帯情報処理装置から、前記接点 A 及び接点 B を介して転送される前記認証用データに基づく認証処理を実行する認証処理ステップを実行し、前記制御ステップは、該認証処理ステップの認証処理結果に基づいてサービスの実行を制御することを特徴とする。

【 0 0 3 2 】

さらに、本発明の認証情報通信方法において、前記サービス提供装置は、さらに、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを有し、前記携帯情報処理装置は、前記認証用ユーザ識別データ生成ステップにおいて生成した認証用ユーザ識別データを前記サービス提供装置から前記接点 B、接点 A を介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納することを特徴とする。

【 0 0 3 3 】

さらに、本発明の認証情報通信方法において、前記認証情報通信方法において、さらに、

ユーザに対する認証処理を実行するユーザ管理ステップを有し、前記ユーザ管理ステップは、ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを生成するステップを含み、前記認証処理は、該登録テーブルに基づいて実行することを特徴とする。

【0034】

さらに、本発明の認証情報通信方法において、さらに、ユーザに対する提供サービスを登録するサービス登録ステップを有し、該サービス登録ステップは、前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを含み、前記携帯情報処理装置は、前記サービス登録ステップにおいて生成された認証用ユーザ識別データを可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納するステップを有することを特徴とする。

【0035】

さらに、本発明の第4の側面は、

人体と接触して人体を介した通信路を形成する接点Aを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Bを有するサービス提供装置とによって実行される認証情報通信システムにおいて、サービス提供装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記接点Bを介して前記携帯情報処理装置に対して、サービス識別データを出力するステップと、

前記サービス識別データに対応する可変ユーザ識別データに基づいて前記携帯情報処理装置が生成した認証用データを前記接点Bを介して受信するステップと

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とするプログラム提供媒体にある。

【0036】

さらに、本発明の第5の側面は、

人体と接触して人体を介した通信路を形成する接点Aを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Bを有するサービス提供装置とによって実行される認証情報通信システムにおいて、携帯情報処理装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記携帯情報処理装置に対して出力されるサービス識別データを前記接点Aを介して受信するステップと、

前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記サービス提供装置に対して、前記接点Aを介して前記認証用データを出力するステップと、

を有することを特徴とするプログラム提供媒体にある。

【0037】

本発明の第4および第5の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0038】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され

、本発明の他の側面と同様の作用効果を得ることができるのである。

【0039】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0040】

【発明の実施の形態】

以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。

【0041】

【実施例1】

本発明の認証情報通信システムの実施例1を構成する送受信装置全体の基本構成を示すブロック図として図1に示す。

【0042】

図1に示すように、本発明の認証情報通信システムは、携帯機器10と、サービス端末20を基本構成とし、携帯機器10とサービス端末20間でのデータ転送を人体を介して実行するものである。携帯機器10は、ユーザ30が保持または装着可能な機器として構成され、例えば腕時計、ネックレス、ブレスレット、指輪等の装身具、またはカード等の部材によって構成することができ、接点18は人体、すなわちユーザ30と接触あるいは導通可能に極めて近接した状態に設定される。

【0043】

サービス端末20は、例えば、街頭あるいは店内などに配置されている音楽情報、映像情報、地図情報、その他、各種の情報提供あるいは商品販売用端末、あるいは銀行に設置されたATM端末、交通機関としての駅の改札ゲート、飛行機、電車その他の公共的乗り物の座席、あるいは建築物の壁に埋設して設置されているような、様々なサービスを提供する装置である。ユーザ30がサービス端末20の接点29に接触、すなわち指を触れたり、手のひらで触れたりすることにより、携帯機器10とサービス端末20の間で通信が可能になる。

【0044】

人体を介する携帯機器10と、サービス端末20間のデータ転送は、携帯機器

10に形成された接点18と、サービス端末20に形成された接点29の両接点に同時に人体、すなわちユーザ30の一部が接触することによって実行される。なお、携帯機器10は例えば腕時計等の装身具であるので、接点18は、基本的に常時人体に接触、あるいは導通可能に極めて近接した状態となっている。従って、ユーザ30がサービス端末20の接点29に触れた時点で、人体を介する携帯機器10とサービス端末20間のデータ転送が実行可能となる。

【0045】

携帯機器10とサービス端末20間のデータ転送は、携帯機器10の通信部15と、サービス端末20の通信部25との間で実行される。この人体を介した通信は、例えば、特開平7-170215に記載の構成が適用できる。人体は、そのほとんどを塩分を含んだ水からなる導電性の容器と考えられるので、数MHz帯では概ね導体となる。なお、テスター等で両手間の直流抵抗を計測すると、手の状態に応じて500kΩから2,3MΩの値を示す。

【0046】

人体の交流における伝達特性を図2に示す。図2(a)は1MHz~20MHz、図2(b)は1MHz~30MHzの範囲で、スペクトラムアナライザを用いて測定した人体の伝送特性(両手間)を示す特性図である。いずれも、トラッキングジェネレータと入力端子に同軸ケーブルを接続した場合の例である。なお、同軸ケーブルのグランドGNDは相互に接続し、アンテナとならないようにした。図2(a)および(b)に示すように、1MHzから20MHz程度の範囲における伝達特性は、概ね平坦で30dBないし40dBの減衰特性となる。

【0047】

図2(a)および(b)に示す測定では、トラッキングジェネレータの出力インピーダンス、スペクトルアナライザの入力インピーダンスとも75Ωである。したがって、もし、交流的にも両手間のインピーダンスが、例えば1メガオームであったとすると、減衰量は-80dBにも達する筈である。ところが、実際には、減衰量は遥かに少なく、人体を介しての信号伝送の可能性を裏付けることが分る。

【0048】

データ送信側は、微小ダイポールアンテナと考えられ、これが発生する電磁界の様子は十分解析されている。それによれば、人体が発生する電磁界は、微小ダイポールアンテナが発生する電磁界となる。電磁界の強さはアンテナからの距離 R 、距離 R の 2 乗、距離 R の 3 乗に反比例する成分のベクトル和で表され、それぞれ、輻射電磁界、誘導電磁界、静電磁界と呼ばれる。なお、これらの関係式については、特開平 7-170215 号に詳しく記載されている。

【0049】

図 3 は電界強度についての図であり、図 3 (a) は、上述した各項の電界強度とアンテナからの距離との関係を示す特性図である。また、図 3 (b) は、周波数 $f = 200 \text{ MHz}$ 、送信端子電圧 $= 100 \text{ dB } \mu\text{V}$ (75Ω) の場合において、 $\lambda/2$ のダイポールアンテナと $3.4 \text{ cm } \phi$ のループアンテナ、および $8 \text{ cm } \phi$ 、 $3.4 \text{ cm } \phi$ のループアンテナの電界強度と距離とを示す図である。図 3 (a) および (b) に示すように、上記輻射電磁界 ($1/R$ 項)、誘導電磁界 ($1/(R \text{ の } 2 \text{ 乗})$ 項)、静電磁界 ($1/(R \text{ の } 3 \text{ 乗})$ 項) の強度は、 $\lambda/2\pi$ の距離において等しくなり、距離がこれ以下の場合には急激に増加する。 $f = 1 \text{ MHz}$ ならば、この距離は約 4.3 m となる。本発明の認証情報通信システムでは静電磁界を主として使用した伝送方式を適用することが好ましい。

【0050】

また、電界強度は、また電波法の EMI (Electromagnetic interference) 規制による制限なく使用可能な範囲を選択することが好ましく、例えば、周波数 332 MHz 以下、電界強度 $500 \mu\text{V}/\text{M}$ 以下とする。

【0051】

上述のように静電磁界は距離 R の 3 乗で減衰する。例えば、距離が 1 m から 3 m になると、電界強度は $1/27$ ($1/(3 \times 3 \times 3)$) になる。従って、データ送信手段からの距離が増加すると、信号強度が極端に減衰するので、複数のユーザが同様の装置を使用している場合であっても他のユーザの信号をノイズとしてとらえる可能性は低くなり、例えば同様の装置を持ったユーザが多数近接して存在する環境下においても、静電磁界を主として使用した通信は良好な通信が可

能になる。

【0052】

なお、携帯機器10に構成される接点18は、広い面積を有することが望ましく、例えば腕時計、ネックレス、指輪、ブレスレット等、曲線状に人体の指、腕、首等に巻き付け可能な構成として、人体の皮膚とより多くの面積で接触する構成とすることが好ましい。

【0053】

携帯機器10は、クレジットカードの認証番号、ATMの暗証番号などのように、個人認証の目的で利用されるIDを記憶する認証用データ記憶部としての固定データ記憶部16、可変データ記憶部17を有している。固定データ記憶部16にはユーザ固有の固定ユーザ識別子が格納される。可変データ記憶部17には、例えば、サービス端末のサービスに応じた識別子等、可変ユーザ識別子が格納される。これらの識別子の態様、および処理については後段で詳細に説明する。なお、固定データ記憶部16と可変データ記憶部17は携帯機器10に対して着脱可能なメモリとして構成してもよい。

【0054】

これらの固定ユーザ識別子、可変ユーザ識別子、あるいはこれらに基づく識別情報が携帯機器10の通信部15からサービス端末20の通信部25に送付されることによって、サービス端末20のCPU21において認証チェックがなされ、サービス端末20の例えばRAM22などに記憶された情報にアクセスすることができ、サービス端末20は、RAM格納情報をサービス端末20の通信部25から携帯機器10の通信部15に送付し、データを受信した携帯機器10は、RAM12等の記憶回路に受信データを蓄えることができる。なお、携帯機器10のROM13やサービス端末20のROM23には、それぞれの装置の基本的な制御を行うOSやデバイスドライバなどの基本ソフトウェアが記憶されており、電源を入れることによってCPUによって読み出されそれぞれの装置を機能させることができる。

【0055】

携帯機器10の電源としては、図示していないが長寿命かつ小型の電源を使用

することが望ましく、例えばリチウム電池バッテリーを使用することができる。CPU 11は、リチウム電池バッテリーからの電源供給を受けてデータの読み出し、データ送信、データ受信、データ蓄積等の各種処理制御を実行する。

【0056】

携帯機器10とサービス端末20との間での通信は、例えばサービス端末20の接点29に人体、すなわちユーザ30の一部が触れたことをサービス端末20に設けた検知手段が検出し、この検出に応じて、サービス端末20から後述するサービス識別子を通信部25、接点29、ユーザ30を介して携帯機器10に出力することにより開始することが可能である。

【0057】

あるいは、サービス端末20の通信部25が連続的に、または数秒毎に、サービス識別子格納手段28に格納されたサービス識別子データを出力する構成としてもよい。この構成における通信部25のデータ出力間隔は、ユーザ30がサービス端末20の接点29に指等を触れる数秒間に少なくとも1回は、送信信号がユーザを介してユーザの携帯する携帯端末10の通信部15によって受信されるような間隔とする。

【0058】

あるいは、上記とは逆に、携帯機器10の通信部15が連続的に、または数秒毎に、固定データ記憶部16、または可変データ記憶部17に記憶されたユーザIDなどの信号を送信する構成としてもよい。この場合もユーザ30がサービス端末20の接点29に指等を触れる数秒間に少なくとも1回は、送信信号がサービス端末20の通信部25によって受信されるような間隔で発生する構成とする。

【0059】

送信信号の種類は、後述するように認証処理においては、例えば、ユーザID、サービス識別子等の認証のために必要なデータである。

【0060】

認証処理後においては、サービス提供端末において、認証に基づく様々な処理が実行される。例えば改札ゲートの開閉処理、ATMの入出金処理、あるいは音

楽情報、画像情報、地図情報、商品情報等の各種コンテンツ情報の提供処理等である。

【0061】

なお、音楽情報、画像情報、地図情報、商品情報等の各種コンテンツ情報の提供を人体を介して転送して携帯機器に蓄積、あるいは付属のディスプレイ等の出力手段で出力する構成としてもよい。なお転送データ中に秘密情報を含む場合は、送信データは、データ送信側で暗号化して、受信側で復号する構成とすることが好ましい。この場合、データ送信側には、例えば、乱数発生手段、タイムスタンプ処理手段等、各種暗号化処理手段を構成する。一方、受信側には、受信した暗号化データを復号する復号手段を構成する。

【0062】

携帯機器10とサービス端末20に構成される通信部は、ユーザ30と各接点18、29との物理的接触により、信号を送受信する。受信信号は各通信部に構成された復調器により復調され、CPU21の制御のもとに、各端末内の回線、あるいは端末外のネットワークを通じて、各記憶手段、情報処理手段、あるいは認証処理手段等に転送される。

【0063】

なお、携帯機器10は、データ送信、データ処理が必要な場合にのみ、CPUに対する電源供給を実行するように構成してもよい。例えば、サービス端末20からの受信信号に基づいて電源供給を開始する構成とすれば、携帯機器10のバッテリー寿命を延ばすことができる。

【0064】

以下、図1に示す認証情報通信システムにおける認証処理、およびデータ転送処理を具体例を示しながら説明する。携帯端末10を装着したユーザ30がサービス端末20に接点29で接触したとする。ユーザ30がはじめてサービス端末20に接触した場合には、認証のための登録処理がなされる。

【0065】

認証登録処理のためにサービス端末20では認証用ユーザ識別子生成部26において認証用のユーザ識別データ（可変ユーザ識別子）を生成し、このユーザ識

別データ（可変ユーザ識別子）をサービス識別子 28 と共に、通信部 25 を経由して携帯端末 10 の通信部 15 に対して送信する。送信されたユーザ識別データ（可変ユーザ識別子）は、携帯端末 10 の可変データ記憶部 17 に記憶される。

【0066】

可変データ記憶部 17 の構成および合成部 14 での処理を説明する図を図 4 に示す。可変データ記憶部 17 は、例えば図 4 に示すようにテーブル構造をなしており、サービス端末 20 から受信したサービス識別子（例えばサービス ID : 101）をキーとするレコードに対して、認証用ユーザ識別子（可変ユーザ ID : 00010011）を格納する構成となっている。

【0067】

携帯機器 10 の合成部 14 は、図 4 に示すようにサービス端末 20 から受信した認証用ユーザ識別子（可変ユーザ識別子（ID）：00010011）と、予め固定データ記憶部 16 に格納されているユーザ固有の固定識別子（固定ユーザ識別子（ID）：10100000）との合成処理を実行する。

【0068】

合成部 14 における合成処理により生成された識別子は、そのユーザ（固定ユーザ ID : 10100000 によって特定される）にのみ有効であり、さらにそのサービス（例えばサービス ID : 101 によって規定されるサービス）にのみ有効な識別子、すなわち特定サービスに有効なサービス固有のユーザ識別子である。

【0069】

携帯機器 10 は、この合成部 14 において生成された特定サービスに有効なサービス固有のユーザ識別子、例えば図 4 右上に記載のサービス : 010 用のユーザ識別子（ID）「10100000 / 00010011」を、サービス端末 20 に対して送信する。携帯機器 10 からサービス端末 20 に対して人体を介して送信されるこのサービス固有のユーザ識別子は携帯機器 10 の接点 18、ユーザ 30、サービス端末 20 の接点 29 を通じてサービス端末 20 の通信部 25 において受信される。

【0070】

サービス端末 20 は受信データを、認証用データ記憶部 27 に記憶する。認証用データ記憶部 27 は、可変データ記憶部 17 と同様の例えばハッシュテーブル構造、すなわち認証用ユーザ識別子としての固定ユーザ識別子をキーとしたテーブル構成を有しており、受信したサービス固有のユーザ識別子をテーブルに記憶する。

【0071】

ユーザ 30 がサービス端末 20 に接触したのが初めてでない場合には、サービス端末 20 が保持するサービス識別子 28 のデータ（例えば 010）を受信した携帯端末 10 は、受信サービス識別子に基づいて可変データ記憶部 17 から受信したサービス識別子に対応する認証用ユーザ識別子（可変ユーザ ID）を取り出して、合成部 14 において、固定データ記憶部 16 に格納されているユーザ固有の固定識別子（固定ユーザ ID）との合成処理を実行してサービス固有のユーザ識別子を生成してサービス端末 20 に送信する。

【0072】

図 4 を用いてこの処理の具体例について説明する。サービス端末 20 の提供するサービス識別子が「010」であったとする。例えばサービス端末 20 がコンビニに設置された情報提供端末であり、サービス識別子が「010」が商品割引券発行サービスであるとする。携帯端末 10（例えば腕時計に内蔵されている）を有するユーザは、コンビニに設置されたサービス端末 20 の接点 29 に指、あるいは手のひらを触れる。サービス端末 20 は、接点 29 に設置されたセンサにより、指、あるいは手のひらの接触を検出し、CPU 21 の制御の下にサービス識別子保持部 25 からサービス識別子「010」を取り出して、これを通信部 25 を介してユーザ 30 に出力する。サービス識別子「010」は、ユーザ 30 の人体を介して、ユーザの皮膚と接点 18 を持つ腕時計型の携帯端末 10 によって受信される。

【0073】

サービス識別子「010」を受信した携帯端末 10 は、可変データ記憶部 17 を検索して、サービス識別子「010」に相当する可変ユーザ ID として「00010011」を取り出し、取り出した可変ユーザ ID「00010011」を

合成部 14 に送る。合成部 14 は、可変ユーザ ID「00010011」と、固定データ記憶部 16 に記憶されている固定ユーザ ID「10100000」とを合成し、「10100000000010011」という特定サービスに有効なサービス固有のユーザ識別子データを得て、これを通信部 15、接点 18、ユーザ 30 の人体、サービス端末 20 の接点 29、を介してサービス端末 20 の通信部 25 に送信する。

【0074】

上述の処理を経て特定サービスに有効なサービス固有のユーザ識別子データを携帯端末 10 から受信したサービス端末 20 は、認証処理を行なう。この認証処理について図 5 を用いて説明する。

【0075】

サービス端末 20 では、携帯端末 10 から送信されるサービス固有のユーザ識別子データ、すなわち上述のデータ「10100000000010011」を受信すると、認証部 24 において、固定ユーザ ID「10100000」と、可変ユーザ ID「00010011」とに分離する処理を行なう。さらに、認証データ記憶部 27 にアクセスして、これらの識別子が認証データ記憶部 27 に登録済みの ID に対応するか否かの確認、すなわち認証処理を行う。正しくデータ照合がなされた場合、すなわち認証がされた場合には、サービス端末 20 に規定されたサービス、すなわち上述のサービス識別子「010」に相当するサービス、例えば商品割引券発行サービスを実行する。サービス端末には、商品割引券発行手段が接続、または内蔵され、この商品割引券発行手段が認証処理に基づいて商品割引券発行処理を開始する。

【0076】

可変ユーザ ID は、例えばサービス端末 20 において商品割引券発行が可能な期間を設定したデータとして構成することができる。この構成とした場合、可変ユーザ ID を受信したサービス端末 20 は、その可変ユーザ ID から有効期間を判定して、有効期間内の場合にのみ正当なサービスを受けるユーザであると判定し、サービスを実行する。また、定期券等の場合は、期間、区間データも併せて可変ユーザ ID 中に登録することで、携帯機器から受信した可変ユーザ ID のみ

からその有効性を判定することが可能となる。

【0077】

サービス端末20が提供するサービスは、例えば入場ゲート、改札、建物の入口、研究室ドアの開閉処理であったり、画像、音声データ等の出力処理、ATMにおける入金、出金処理等、様々なサービスである。サービスが改札ゲートの開閉である場合は、上述の認証処理に基づいて、改札がオープンし、認証されたユーザのみが改札を通ることができる。この場合、サービス端末20の接点29は各改札ゲートに設置される。

【0078】

なお、サービス端末20は、複数のサービス識別子を保持し、各々のサービス識別子に対応してサービス固有のユーザ識別子データを格納したテーブルを保持する構成とすることにより、各個人に対して異なるサービスを提供することが可能である。

【0079】

なお、上述の例では、固定ユーザIDと可変ユーザIDとを単純に連結したデータを合成データとして生成し、これをサービス固有のユーザ識別データとする例を説明したが、サービス固有のユーザ識別データの生成は、上述した方法に限らず、固定ユーザIDと可変ユーザIDに基づいて予め定めた関数等により新たなデータ列を生成してサービス端末20に送信し、サービス端末20がこれを解読する構成としてもよい。これらの関数処理、解読処理は、例えば暗号化処理、復号処理の組合わせとしてもよい。また、可変ユーザIDのみをサービス端末20に出力して、サービス端末20が可変ユーザIDのみに基づいて認証処理を実行してユーザの識別及びサービスの実行可否を決定するように構成してもよい。サービス端末20は、サービスに応じてユーザに可変ユーザIDを設定する構成であるので、可変ユーザIDのデータにユーザ個々の情報、提供サービスの情報、制限等、各種情報を含ませることが可能になる。

【0080】

サービス端末20が情報提供を行なう端末である場合、認証処理に基づいて提供する音楽情報、画像情報等、様々な情報は、サービス端末20に設けたディスク

プレイ等の表示手段に表示してもよく、さらに、携帯機器に付属して設けたディスプレイ等の出力手段に、上述の認証データと同様に人体を介してサービス端末から画像情報等を転送して、ユーザに提供する構成としてもよい。なお、人体を介した画像、音声情報等の伝送態様については、本出願と同一出願人による先の特許出願（特開平7-170215号）に詳細に説明されている。

【0081】

携帯端末10の例を図6に示す。図6（a）は、ブレスレット601に接点を設けて、内部に図1に示す携帯機器10としての構成を内蔵したものである。図6（b）は、ネックレス602に接点を設けて、内部に図1に示す携帯機器10としての構成を内蔵したものである。図6（c）は、指輪603に接点を設けて、内部に図1に示す携帯機器10としての構成を内蔵したものである。図6（d）は、腕時計604に接点を設けて、内部に図1に示す携帯機器10としての構成を内蔵したものである。ブレスレット601、ネックレス602、指輪603、および腕時計604の接点は、それぞれ人体と接触する側、すなわち内周側に設けられ、各接点を介して、ユーザである人体、さらにユーザの指、手のひら等、図1に示すサービス端末20の接点29に触れた人体の物理的接触点を介して携帯機器10とサービス端末20との間のデータ転送が可能になる。このように、携帯端末10は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレット等、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有する。

【0082】

次に、図7～9を用いて本発明の認証情報通信システムにおける認証処理フローについて説明する。図7は、図1に示す認証情報通信システムにおける携帯機器10の処理フローであり、図8および図9は、図1に示す認証情報通信システムにおけるサービス端末20の異なる態様での処理フローを示す。

【0083】

まず、図7の携帯機器10の処理フローについて説明する。ステップ701はデータ受信のため、接点18の電位上昇を確認するステップであり、データ受信に必要な電位を閾値として接点18の電位を判定するステップである。接点電位がデータ受信可能状態になると、ステップ702において、サービス端末20か

らユーザ30の人体を介して送られるサービスIDを受信する。

【0084】

サービスIDを受信した携帯端末10は、ステップ703において、受信したサービスIDに対応する可変ユーザIDを可変データ記憶部17から取り出し、さらに固定データ記憶部16から固定ユーザIDを取り出して合成部14において合成処理を行ない、認証用IDを生成し、ステップ704において、生成した認証用IDをサービス端末20に対して人体を介して出力する。

【0085】

認証用IDをサービス端末20に出力した携帯端末10は、ステップ705において受信側、すなわちサービス端末からの承認応答を待つ。承認応答を受信した場合は、サービス端末20からのさらなる処理要求を待機（ステップ706）し、要求があった場合は、ステップ707において処理を実行する。

【0086】

この図7に示すフローは特定のサービス端末、例えば銀行のATM等を想定した場合の処理フローである。図7のフローにおけるステップ705以降の処理は、サービス端末の態様によって異なるものとなる。サービス端末20が銀行端末である場合、例えば、ステップ705の承認応答は、ステップ704での出力IDに基づく認証がなされた後のディスプレイへの承認表示処理に相当し、ステップ706の処理要求は、例えば引き出し金額の指定要求であり、ステップ707の処理実行は、ユーザによる金額指定の処理等に対応する。

【0087】

また、サービス端末が改札ゲートであるとする、ステップ704において、ユーザの携帯機器から認証用IDの出力がなされると、サービス端末である改札ゲートに接続された端末は、認証の可否に基づいて改札ゲートの開閉を実行することになる。このように、図7の処理フローはサービス端末の提供する処理に応じて異なるものとなる。

【0088】

次に、図8に基づいてサービス端末側での処理例について説明する。図8の例は、駅の改札のように機器の動作を処理するだけのサービスの例である。ステッ

ブ 801 はデータ送信のため、接点 29 の電位上昇を確認するステップであり、データ送信に必要な電位を閾値として接点 29 の電位を判定するステップである。接点電位がデータ送信可能状態になると、ステップ 802 において、サービス端末 20 からユーザ 30 の人体、接点 29 を介して携帯機器 10 に対してサービス ID を送信する。

【0089】

サービス ID を受信した携帯機器 10 は、受信したサービス ID に対応する可変ユーザ ID を可変データ記憶部 17 から取り出し、さらに固定データ記憶部 16 から固定ユーザ ID を取り出して合成部 14 において合成処理を行ない、認証用 ID を生成し、生成した認証用 ID をサービス端末 20 に対して出力する。サービス端末 20 は、携帯機器 10 からの認証用 ID を受信すると（ステップ 803）、ステップ 804 で、受信認証用 ID の認証処理を実行する。この処理は、図 1 における認証部 24 が実行する。認証部 24 における認証の結果、認証用 ID の正当性が判定（ステップ 805）され、正当であると判定されると、ステップ 806 においてサービス端末に設定されたサービスが実行される。一方、ステップ 805 における判定処理で、正当でないと判定されると、ステップ 807 に進み、サービスは中止され、処理が終了する。

【0090】

次に、図 9 に基づいてサービス端末側での異なる処理例について説明する。図 9 の例は、情報端末のように画像情報、音楽情報等、各種情報を提供するサービスの場合の処理例である。ステップ 901 はデータ送信のため、接点 29 の電位上昇を確認するステップであり、データ送信に必要な電位を閾値として接点 29 の電位を判定するステップである。接点電位がデータ送信可能状態になると、ステップ 902 において、サービス端末 20 から接点 29、ユーザ 30 の人体を介して携帯機器 10 に対してサービス ID を送信する。

【0091】

サービス ID を受信した携帯機器 10 は、受信したサービス ID に対応する可変ユーザ ID を可変データ記憶部 17 から取り出し、さらに固定データ記憶部 16 から固定ユーザ ID を取り出して合成部 14 において合成処理を行ない、認証

用IDを生成し、生成した認証用IDをサービス端末20に対して出力する。サービス端末20は、携帯機器10からの認証用IDを受信すると（ステップ903）、ステップ904で、受信認証用IDの認証処理を実行する。この処理は、図1における認証部24が実行する。認証部24における認証の結果、認証用IDの正当性が判定（ステップ905）され、正当でないと判定されると、ステップ909においてサービスが中止され、処理を終了する。ステップ905において認証用IDが正当であると判定されると、ステップ906においてサービス端末に設定されたサービスに規定された処理要求を出力する。さらに、ステップ907において、処理要求に対する応答を待機し、応答があった場合は、ステップ908において処理を実行し、要求データの送信を行なう。

【0092】

上述の図8、図9のサービス端末の処理において、例えば図8のフローは、ビルでのセキュリティチェック・サービスの例に相当する。この場合、ステップ806のサービスは、ビルのドアの開閉の制御になり、ステップ807のサービス中止はドアの開閉処理の中止を意味する。さらに、ステップ807のサービス中止に伴う処理として不当IDを登録するといった処理を行う構成としてもよい。

【0093】

また、図8の処理フローは、交通システム精算サービスの例に相当し、この場合ステップ806のサービスは改札ゲートの開閉をコントロールするだけでなく、料金精算が必要な場合には、電子精算処理も行う構成とすることができる。

【0094】

また、図8の処理フローは、携帯電話、ディスプレイを有する携帯端末の利用携帯としても適用可能である。例えば、図10に示す（a）携帯電話や、（b）PDA等のディスプレイ機器などを利用した処理が可能である。ここで図10（a）の携帯端末は導電性の接点を具備することを特徴とするサービス端末であり、図10（b）ディスプレイ端末は、導電性のあるジョグダイヤルを具備することを特徴とするサービス端末である。

【0095】

図10（a）の携帯電話において、図8のサービス端末の処理を実行する場合

、サービス端末としての携帯電話を複数人で使う利用形態において、ユーザの識別データを腕時計等の携帯機器から携帯電話にユーザの人体を介して転送し、認証用IDの正当性が確認された場合のみ携帯電話の使用が可能となる構成が実現される。この場合の図8のステップ806のサービスは通話可能モードへの設定処理となる。なお、携帯電話のディスプレイ領域に認証用IDに相当する電話番号リストを表示するようにしてもよい。また、図10(b)のPDA等のディスプレイ機器の場合には、オンラインショッピングを行う場合に、認証用IDをベースにして、サービスプロバイダとの認証を行い決裁を行うシステムとしての利用が考えられる。

【0096】

さらに、図9に示した処理フローを実行するサービス端末の例としてリモート機器制御機器がある。例えば、病院等では電波を発生するために携帯電話の使用が制限されている。このような状態で、ベッドから移動することができないような患者に対して、電話機器を利用することができるようなサービスを提供する端末が実現される。

【0097】

図11を用いて図9に示した処理フローを実行するサービス端末の例について説明する。患者40が表示部を持つ腕時計タイプの携帯機器41を身につける。患者40が電話をかけたいときは、壁から吊り下げられたワイヤー状の接点42に触れることにより、壁43に埋め込まれたサービス端末44あるいは、壁43を通じて遠隔地に存在するサービス端末44と通信を行う。

【0098】

患者40がワイヤー状の接点42を持つことにより、サービス端末44からサービスIDが送信(ステップ902)され、これに応答して、携帯機器41から認証用IDが携帯機器に送られて、サービス端末44において認証用IDの正当性チェックが実行(ステップ904)される。

【0099】

認証処理で正当性が確認されると、処理要求、すなわち、電話番号データの出力を患者40に要求(ステップ906)する。電話番号データは、患者による音

声出力、あるいは携帯機器 41 に構成した電話番号データ入力キー等によって行なうことが可能な構成とし、これらの電話番号を受信したサービス端末 44 は、電話を接続する処理を実行（ステップ 908）する。この構成において、サービス端末 44 には、モデムの機能が内蔵されている。サービス端末 44 はさらに構内回線 45 を通じてデジタル交換器 46 と接続しており、この交換器 46 から外部公衆回線網 47 を通じて外部に電話をかけることが可能となる。

【0100】

サービス端末 44 が留守番電話の機能を有するようにすれば、患者がワイヤ状の接点 42 を持つことにより、その情報を携帯機器 41 に受信し、接点 42 を離れた後で、携帯機器 41 の再生機能を使って、情報を再生することも可能である。

【0101】

〔実施例 2〕

次に図 12 に示すように、認証情報通信システムが、ユーザ 30 が装着した携帯機器 100 と、サービス提供端末 110 と、サービス登録端末 120、並びに認証課金等のユーザ管理を行うのためのクリアリングハウス 130 とから構成されたシステム構成例について、第 2 実施例として説明する。

【0102】

図 12 に示すシステムは、サービス提供端末 110 からのサービスを受けるユーザに対して、ユーザの認証処理のみならず、ユーザ毎に使用可能なサービスを設定するとともに、サービス利用状況を把握して、ユーザ単位の課金を可能としたシステムである。

【0103】

サービス提供端末 110 は、実際のサービスを提供する端末、例えば、音楽、画像情報等のコンテンツ情報の提供端末、あるいは遊園地の改札ゲート、駅の改札ゲート等、様々な場所に設置された様々なサービスを提供する端末である。なお、図 12 には、サービス端末 110 が 1 つのみ記載されているが、サービス端末 110 はネットワーク 140 を介して複数台、必要な位置、例えばサービス端末が改札ゲートの開閉処理を実行する場合はそれぞれのゲート位置に配置されて

いるものであり、図 12 では、複雑化を避けるために 1 つの構成のみを記載していることを理解されたい。

【0104】

サービス提供端末 110 の CPU 111 は、RAM 113 格納情報をサービス提供端末 110 の通信部 2, 115 から携帯機器 100 の通信部に送付し、データを受信した携帯機器 100 は、携帯機器 100 内の RAM 等の記憶回路に受信データを蓄えることができる。なお、通信部 1, 114 は、サービス登録端末 120、クリアリングハウス 130 との通信用である。さらに、サービス提供端末 110 の ROM 112 には、それぞれの装置の基本的な制御を行う OS やデバイスドライバなどの基本ソフトウェアが記憶されており、CPU 111 によって読み出されそれぞれの装置を機能させることができる。

【0105】

サービス登録端末 120 は、ユーザ 30 が、サービス提供端末 110 からのサービスを受けるために必要な登録を行なうための端末であり、例えばサービス提供端末 110 が駅の改札ゲートであれば、サービス登録端末 120 は定期券、切符等の販売を行なう駅に設置され、サービス提供端末 110 が遊園地の改札ゲートであればサービス登録端末 120 は入場券販売所等に設置される。また、サービス登録端末 120 が音楽、画像情報等のコンテンツ情報の提供端末であれば、サービス登録端末 120 は、例えばコンビニエンスストアや駅などに設置されている情報提供端末、ATM のような装置として構成することができる。

【0106】

サービス登録端末 120 の CPU 121 は、RAM 123 格納情報をサービス登録端末 120 の通信部 2, 125 から携帯機器 100 の通信部に送付し、データを受信した携帯機器 100 は、携帯機器 100 内の RAM 等の記憶回路に受信データを蓄えることができる。なお、通信部 1, 124 は、サービス提供端末 110、クリアリングハウス 130 との通信用である。サービス登録端末 120 の ROM 122 には、それぞれの装置の基本的な制御を行う OS やデバイスドライバなどの基本ソフトウェアが記憶されており、CPU 121 によって読み出されそれぞれの装置を機能させることができる。

【0107】

サービス登録端末120は、登録処理のための入出力機器、例えば、情報出力、入力用のディスプレイ、マイク、スピーカ等を備えている。携帯機器100を装備したユーザ30は、サービス登録端末120との通信においてもサービス登録端末120に設定された接点128を介した通信を実行する。携帯機器100を装着したユーザ30が接点128においてサービス登録端末120に接触し、サービス登録端末120の接点128の電位が上昇し、通信可能な状態になると、サービス登録端末120は、まずユーザに対して、サービスの選択処理を実行することを要求する。

【0108】

サービス登録端末120のサービス選択部127は、ユーザに対してサービス登録端末120に構成されたディスプレイ、またはサービス登録端末120に接続されて配置されたディスプレイに図13に示すようなメッセージ201を表示し、選択画面202中のサービス項目の中の一つを選択するように促す。

【0109】

ユーザ30が、図13に示すディスプレイの選択画面202からタッチ入力、あるいはキーボード入力、音声入力、その他の入力手段によりサービス項目の一つを選択すると、サービス登録端末120は、ユーザ30に対してユーザ30の選択したサービスに対応するサービス識別子を通信部2、125、接点128を介して、ユーザ30の装着した携帯機器100に送付する。

【0110】

サービス識別子を受信したユーザ30の携帯機器100は、実施例1と同様に、可変データ記憶部17（図1、図4参照）で可変ユーザIDを選択する。このとき、ユーザ30が以前に一度も当該サービスを利用していなければ、この可変ユーザIDは初期化された値（例えば0）になっている。

【0111】

さらに、ユーザ30の携帯機器100の合成部14（図1、図4参照）で固定データ記憶部のデータ、すなわち予めユーザに対する固定値として設定されている固定ユーザIDと先述した可変データ記憶部17に記憶されたサービスに対応

する可変ユーザIDが合成されて生成されたサービス固有のユーザ識別子が、サービス登録端末120に送信され、通信部2、125において受信される。

【0112】

次にサービス登録端末120は、通信部1、124を使ってクリアリングハウス130と通信を行うことにより、ユーザ30の認証処理を行う。

【0113】

クリアリングハウス130は、サービス提供端末110と、サービス登録端末120との通信を実行する通信部1、134、基本的な制御を行うOSやデバイスドライバなどの基本ソフトウェアが記憶されたROM132、CPU131によって実行されるプログラムのワークエリアと、入力されたデータなどを一時的に記憶するRAM133を有し、ユーザ30の認証処理を実行する。ユーザ30の認証処理は、インターネット、あるいはその他の通信回線140を介してクリアリングハウス130の通信部1、134がユーザ30の認証用データを受信し、受信したデータを認証部135に送り、ここで前述の図4によって説明したと同様の処理を実行して認証処理を行う。

【0114】

認証処理は、この実施例では、クリアリングハウス130の課金認証データ記憶部136に記憶された登録テーブルを用いて行なう。クリアリングハウス130の課金認証データ記憶部136は、例えば図14に示されるようなデータ構造の登録テーブルを有しており、登録テーブルにユーザ毎の最大使用度数、現在使用度数をセットする構成となっている。図14に示す登録テーブル14は一例であり、サービス態様に応じた項目、例えば個々のユーザに設定されたサービス使用期間、サービス使用時間、サービス使用地域、その他のサービスの詳細についての項目を、提供するサービスに応じて設定する。

【0115】

ここで、図14に示す登録テーブルを使用した場合には、ユーザごとの課金認証データ記憶部136の登録テーブルの状況として、以下の3つの態様が考えられる。

(1) ユーザ30は既になんらかのサービスを過去に使った履歴があり、固定ユ

ーザIDが一致するレコードが課金認証データ記憶部136に存在しているが、今回の要求サービスに対応するレコードは存在しない。

(2) ユーザは、今回要求したサービスと同じサービスを過去に利用したことがあるので、対応する固定IDレコードが存在する。

(3) ユーザは一度もサービスを利用したことがないので、ユーザのIDは登録されていない。

【0116】

上述の各態様において、(1)または(3)の場合は、ユーザ30から要求のあったサービスに対してユーザ登録が新たに必要となるので、登録処理要求をサービス登録端末120に通知し、サービス登録端末120は、ユーザ30から要求のあったサービスに対するユーザ登録処理を実行する。具体的には、ユーザ識別子生成部126において当該ユーザに対応するユーザ識別子(可変ユーザ識別子)を生成し、当該サービスのサービス識別子とともに、通信部2, 125から接点128、ユーザ30を介してユーザの携帯端末100に送信する。ユーザ30の携帯端末100では、受信したサービス識別子と可変ユーザ識別子との対を可変データ記憶部17に対応させて記憶する(図4参照)。

【0117】

サービス識別子と、このサービス識別子に対応する可変ユーザ識別子とを、携帯機器100の可変データ記憶部17に登録したユーザは、その後、携帯端末100の合成部14で、固定データ記憶部の固定ユーザ識別子と今受信した可変ユーザ識別子とを合成し、サービス固有のユーザ識別子を生成して、これをサービス登録端末120に送付することによって、サービス登録端末120にユーザ登録処理の実行を依頼する。

【0118】

ユーザ登録依頼を受け取ったサービス登録端末120は、次にクリアリングハウス130に対して、受信したサービス固有のユーザ識別子を転送することにより、ユーザ登録を依頼する。このサービス固有のユーザ識別子データを受信したクリアリングハウス130は、自身の課金認証データ記憶部136に対して、当該サービス固有のユーザ識別子に相当するレコードを作成し、最大使用度数を所定

の数値にセットすると共に、現在使用度数を0として初期化する。

【0119】

上述の手続きを実行し、ユーザ登録が完了したユーザ30は、サービス固有のユーザ識別子を携帯機器100の可変データ記憶部に保持することになり、要求したサービスをサービス提供端末110を介して受けることができる。

【0120】

サービス提供を受けようとするユーザ30は、サービス提供端末110の接点116に触れ、サービス提供端末110から、接点116、ユーザ30の人体を介して携帯機器100に対するサービス識別子の転送を受ける。携帯機器100は、これに応答して、登録した可変ユーザIDと固定ユーザIDを合成し、サービス固有のユーザ識別子を生成して、これをサービス提供端末110に転送する。

【0121】

さらに、このサービス固有のユーザ識別子が、クリアリングハウス130にネットワーク等を介して転送されて、認証処理、および課金認証データ記憶部136の登録テーブルの使用度数の更新が行なわれる。認証処理は、前述の実施例と同様の処理となる。ユーザ30は、このような手続きを経て、使用度数に至るまでサービス提供端末110からのサービスを受けることができる。

【0122】

次に(2)の場合、すなわち、今回要求したサービスと同じサービスを過去に利用したことがあり、対応する固定IDレコードが登録テーブルに存在する場合の処理について説明する。(2)の場合は、さらに、次の2つのケースが考えられる。(2-1)まだ現在使用度数が最大使用度数を超えていない。(2-2)すでに現在使用度数が最大使用度数を超えている。

【0123】

(2-1)の場合には、クリアリングハウス130は、サービス登録端末120に対して、「登録の必要がない」という意味のメッセージを送付する。サービス登録端末120は、このメッセージを受信することにより、ユーザ30に対して、その旨通知して、処理を終了する。(2-2)の場合には、クリアリングハ

ウス130は、サービス登録端末120に対して、「更新の必要あり」という意味のメッセージを送付する。サービス登録端末120は、このメッセージを受信することにより、ユーザ30に対して、その旨通知して、ユーザ30に対して、更新するかどうかの問い合わせを行う。ユーザ30が更新に同意する場合には、クリアリングハウス30に対して、更新処理を依頼する。

【0124】

クリアリングハウス30における更新処理は、具体的には、例えば、課金認証データ記憶部136の登録テーブルの対応するレコードの現在使用度数を0にセットする処理である。ユーザ30が更新に対して同意しない場合には、さらにユーザ30に対して、課金認証データ記憶部136の登録テーブルのレコードを削除するかどうかの問い合わせを行う。ユーザ30がレコード削除に同意した場合には、クリアリングハウス30に対して、当該レコードの削除を依頼し、クリアリングハウス30は当該レコードを課金認証データ記憶部136から削除する。ユーザ30がレコード削除に同意しない場合には、サービス登録端末120はそのまま処理を終える。

【0125】

携帯端末100を所持するユーザ30が、サービス提供端末110に接点116で接触してサービスの提供を受ける場合の処理について説明する。サービス提供端末110にはサービスを提供するためのデータ入出力機器としての表示ディスプレイ118、マイク119が付属しており、サービス開始の際には、表示ディスプレイ118に、例えば図15に示すような案内表示がなされる。表示ディスプレイにはサービス選択画面301が示される。

【0126】

ユーザ30がサービス提供端末110の接点116に接触すると、サービス提供端末110は、サービス識別子記憶部117のデータを読み出し、ユーザ30の携帯端末100に対してサービス識別子を通信部2, 115、接点116、ユーザ30の人体を介して送信する。

【0127】

図4を用いてこのサービス識別子受信後の処理を説明する。サービス識別子が

「010」であったとする。この場合、携帯機器100の可変データ記憶部17においてサービス識別子「010」に相当するレコードには可変ユーザ識別子として「00010011」が記憶されているので、これを、固定データ記憶部16に記憶されている固定ユーザ識別子「10100000」と合成部14において合成処理を実行し、例えば、「10100000000010011」というデータを生成する。

【0128】

このデータは、サービス固有のユーザ識別子であり、これをサービス提供端末110に送付する。当該データを受信したサービス提供端末110は、その後このデータをクリアリングハウス130に送付することによって、ユーザ認証・課金処理を依頼する。クリアリングハウス130では、サービス提供端末110から送信されたサービス固有のユーザ識別子データを受信すると、認証部135において、サービス固有のユーザ識別子に基づいて、固定ユーザ識別子「10100000」と可変ユーザ識別子「00010011」を分離生成する処理を実行したのち、課金認証データ記憶部136にアクセスしてユーザが登録されているかどうかの認証を行う。

【0129】

その後、課金認証データ記憶部136にて図14にあるような登録テーブルを用いて認証が正しくなされた場合には、サービス提供端末110に対して「認証OK」のメッセージを送信すると同時に、課金認証データ記憶部の当該レコードの現在使用度数を1減少させる。クリアリングハウス130から「認証OK」のメッセージを受信したサービス提供端末110では、サービスが提供される。

【0130】

クリアリングハウス130において認証が失敗した場合には、サービス提供端末110に付属するディスプレイ装置118等に「認証が失敗した」旨を通信するメッセージを表示することによって、処理を終了する。

【0131】

以上の例において、通信中のデータの安全性を考慮して、各構成要素の通信部1, 114, 通信部2, 115, 通信部1, 124, 通信部2, 125, 及び通

信部 1, 134 から送出されるデータは暗号化装置によって暗号化されて送出されるようにし、各通信部において受信された後に復号するようにしてもよい。

【0132】

上述の例は、サービス提供端末 110 がディスプレイを使用した情報提供を主に実行する構成の例であるが、ユーザの受けようとするサービスが駅、遊園地等の改札ゲートの開閉動作であってもよく、この場合、サービス提供端末 110 は、各駅、あるいは遊園地の複数の場所に設置された改札ゲートとして構成される。この場合、図 12 のサービス提供端末 110 は、各ゲートに対応して配置される。ユーザ 30 はサービス提供端末 110 の接点 116 に触れ、合成処理により生成されたサービス固有のユーザ識別子、この場合は、定期券の所定区間、所定期間に対応する改札開閉処理サービス固有のユーザ識別子をサービス提供端末 110、クリアリングハウスに転送し、認証処理、課金または清算処理を行ない、有効な認証処理がなされた場合のみ、改札ゲートをオープンさせる。

【0133】

認証処理は先に説明したように、ユーザの装着した携帯機器 100 とサービス提供端末とのユーザ 30 を介した通信を実行して行われる。従って、接点 116 は、各ゲートに設置された接点である。携帯機器 100 を装着したユーザ 30 が接点 116 を触れることで、認証処理が実行され、認証がなされた場合は、ゲートがオープンする。

【0134】

この場合、サービス登録端末 120 は、ユーザ 30 がサービスを受けるために必要な登録を行なうための端末であり、定期券、切符等の販売を行なう駅、あるいは、入場券販売所等に設置される。

【0135】

サービス登録端末 120 での登録処理は、ユーザ 30 がサービス登録端末 120 の接点 128 に触れることによって開始される。サービス登録端末 120 において、ユーザ 30 は、特定のサービス、例えば、定期券の販売であれば、駅区間、有効期間の設定を行ない、これらの設定区間、期間のデータを前述のクリアリングハウス 130 の課金認証データ記憶部 136 の登録テーブル中に登録し、登

録テーブルを参照してユーザの認証処理を実行する。このように、サービス提供端末の提供するサービスは各種可能であり、サービス単位、かつユーザ単位の認証処理、管理が可能となる。

【0 1 3 6】

なお、以上の説明では、基本的に認証を行う携帯機器についての例を述べたが、認証が不要な応用例、例えば、本携帯機器の認証機能をオフ、あるいはすべてのユーザを無条件に認証するとした設定とすることで、情報交換機器としても利用、すなわち外部情報入力システムとしての応用が可能である。例えば、電車内での所定の位置、例えば、公告の一部、または吊革等に接点を構成することで、携帯機器を有するユーザがこれらの接点に接触することで、電車内の広告情報が携帯機器に入力されるようにすることができる。携帯機器中のメモリに情報を取り込んだり、あるいは携帯機器に付属するディスプレイ、スピーカを通じて情報を出力する構成としてもよい。

【0 1 3 7】

さらに、図 1 6 のように、腕時計型あるいはブレスレット型の携帯装置 2 0 1、2 0 2 を装着した 2 人のユーザが、携帯装置 2 0 1、2 0 2 をそれぞれ装着して握手を行なうことにより、携帯装置 2 0 1 と携帯装置 2 0 2 の間で、握手した人体を介するデータ転送を行なうことが可能である。また、携帯装置 2 0 1 と携帯装置 2 0 2 内に認証処理構成を内蔵させれば、認証された携帯機器を有する者同士では、情報を転送することが可能であるが、認証されない相手に対しては、情報の転送が実行されない構成とすることができる。

【0 1 3 8】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0 1 3 9】

【発明の効果】

以上の説明から明らかなように、本発明の認証情報通信システムおよび認証情報通信方法によれば、ユーザが装着した携帯機器と、サービスを提供するサービス提供端末間での認証処理を人体を介する通信によって実行し、それぞれの接点に人体が触れることでデータ通信を可能としたので、ユーザが接触したという物理的実感を確認して認証処理が行なわれ、非接触型の認証システムにおける処理の開始確認の曖昧さが解消され、ユーザの不安感が取り除かれるとともに、またカード等の旧来の接触型の認証システムのようなカードの取り出し、センサでの読み取り処理等のわずわらしさもなく、ユーザの負担が軽減される優れた認証処理システムが実現される。

【0140】

さらに、本発明の認証情報通信システムおよび認証情報通信方法によれば、ユーザが装着した携帯機器にユーザ固有のユーザ固有識別子と、サービス端末の提供するサービスに応じて各ユーザごとに生成されるユーザ可変識別子とを格納し、サービス端末から送信されるサービス識別子に応じて、携帯端末において、ユーザ固有識別子とユーザ可変識別子とから認証用のサービス固有ユーザ識別データを生成してサービス端末に送付する構成としたので、サービス識別子で規定した内容に応じたユーザ単位の課金処理等、様々なユーザ管理、サービス管理が実行できる認証処理システムが実現される。

【0141】

さらに、本発明の認証情報通信システムおよび認証情報通信方法によれば、サービス端末がサービスに応じた可変ユーザIDをユーザに対して設定する構成としたので、可変ユーザIDのデータにユーザ個々の情報、提供サービスの情報、制限等、各種情報を含ませることが可能になり、携帯機器から受信した可変ユーザIDに基づいてサービスの実行、態様を変更することが可能となる。

【図面の簡単な説明】

【図1】

本発明の認証情報通信システムの基本構成を示すブロック図である。

【図2】

1MHz～30MHzの範囲でスペクトラムアナライザを用いて測定した人体

の伝送特性（両手間）を示す特性図である。

【図 3】

電解強度とアンテナからの距離との関係を説明する特性図である。

【図 4】

本発明の認証情報通信システムの認証処理におけるユーザ側の携帯機器における処理を説明する図である。

【図 5】

本発明の認証情報通信システムの認証処理におけるサービス端末における処理を説明する図である。

【図 6】

本発明の認証情報通信システムにおける携帯機器の機器構成例を示す図である。

【図 7】

本発明の認証情報通信システムにおける携帯機器における処理フローを説明する図である。

【図 8】

本発明の認証情報通信システムにおけるサービス端末における処理フロー（その 1）を説明する図である。

【図 9】

本発明の認証情報通信システムにおけるサービス端末における処理フロー（その 2）を説明する図である。

【図 10】

本発明の認証情報通信システムの使用例（その 1）を説明する図である。

【図 11】

本発明の認証情報通信システムの使用例（その 2）を説明する図である。

【図 12】

本発明の認証情報通信システムにおける第 2 実施例の構成を示すブロック図である。

【図 13】

本発明の認証情報通信システムにおける第 2 実施例のサービス登録端末での処理例を示す図である。

【図 1 4】

本発明の認証情報通信システムにおける第 2 実施例の課金認証データ記憶部の登録テーブルの例を示す図である。

【図 1 5】

本発明の認証情報通信システムにおける第 2 実施例のサービス提供端末での処理例を示す図である。

【図 1 6】

本発明の認証情報通信システムにおけるその他の実施例の使用例を示す図である。

【符号の説明】

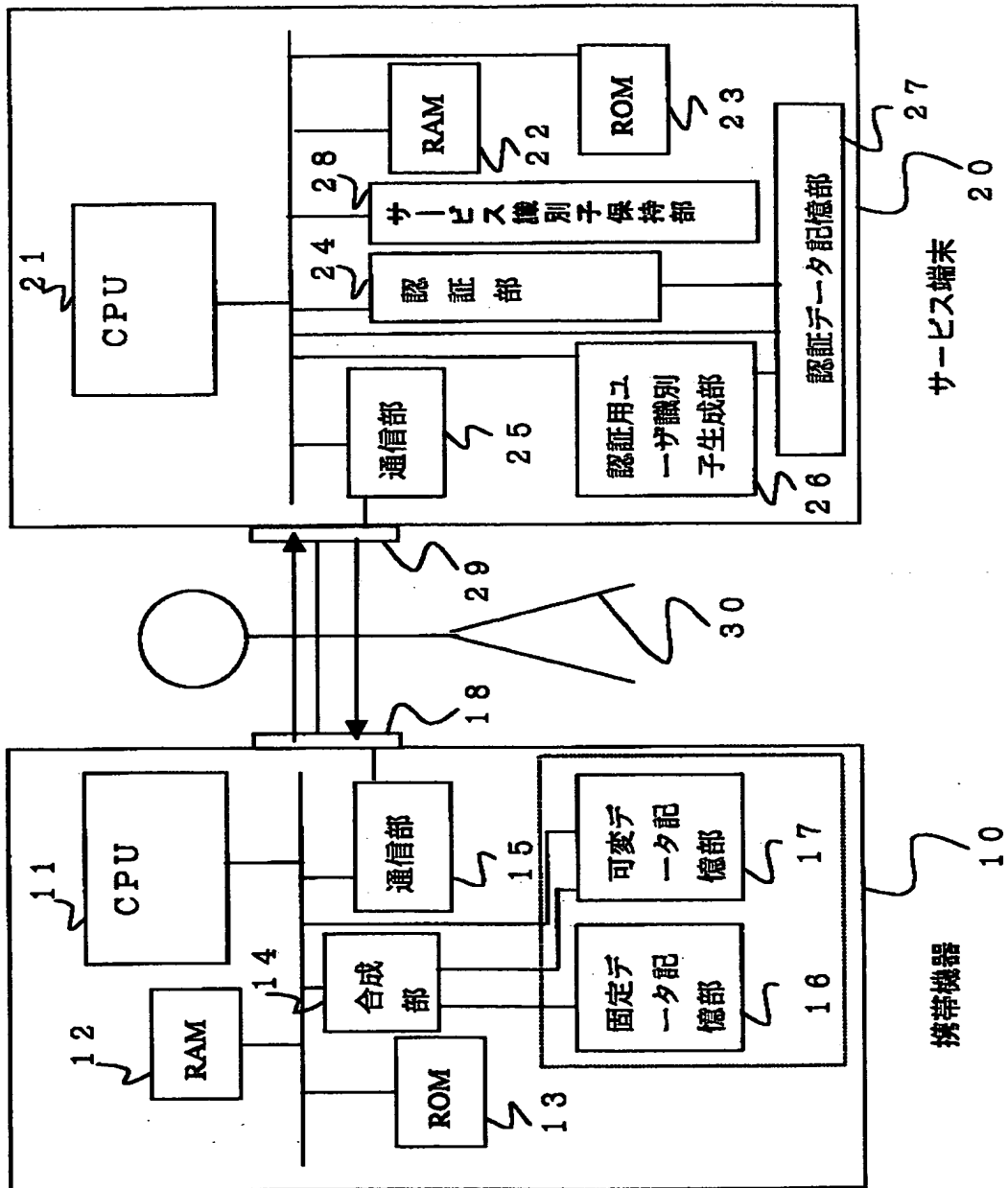
- 1 0 携帯機器
- 1 1 CPU
- 1 2 RAM
- 1 3 ROM
- 1 4 合成部
- 1 5 通信部
- 1 6 固定データ記憶部
- 1 7 可変データ記憶部
- 1 8 接点
- 2 0 サービス端末
- 2 1 CPU
- 2 2 RAM
- 2 3 ROM
- 2 4 認証部
- 2 5 通信部
- 2 6 認証用ユーザ識別子生成部
- 2 7 認証データ記憶部

2 8 サービス識別子保持部
4 1 携帯機器
4 2 接点
4 4 サービス端末
4 6 交換機
1 1 0 サービス提供端末
1 1 6 接点
1 1 7 サービス識別子記憶部
1 2 0 サービス登録端末
1 2 6 ユーザ識別子生成部
1 2 7 サービス選択部
1 2 8 接点
1 3 0 クリアリングハウス
1 3 5 認証部
1 3 6 課金認証データ記憶部
2 0 1, 2 0 2 携帯装置

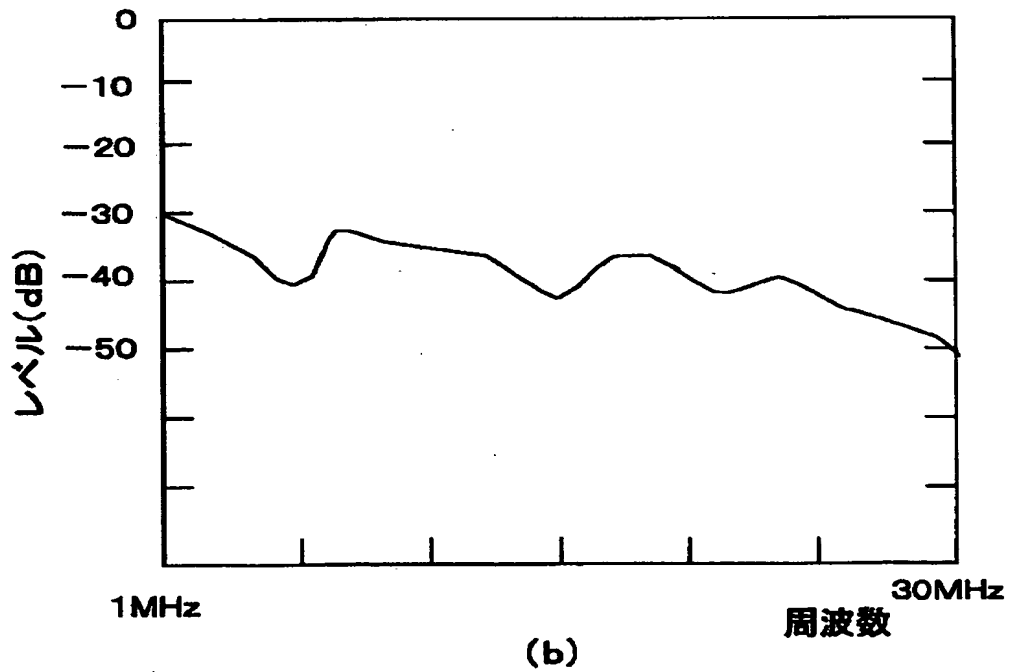
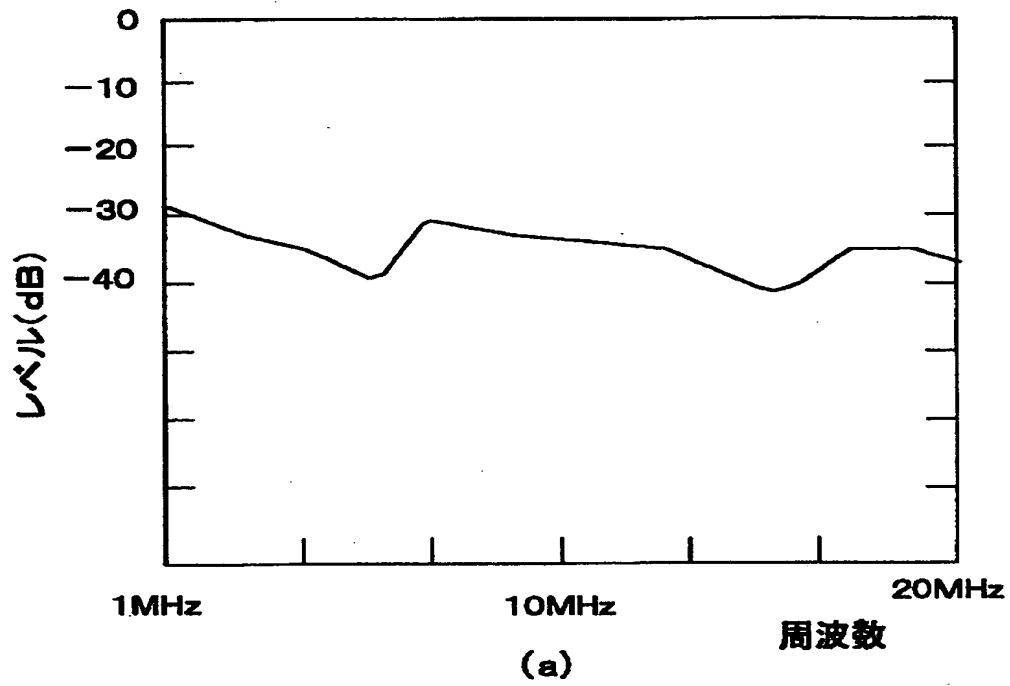
【書類名】

図面

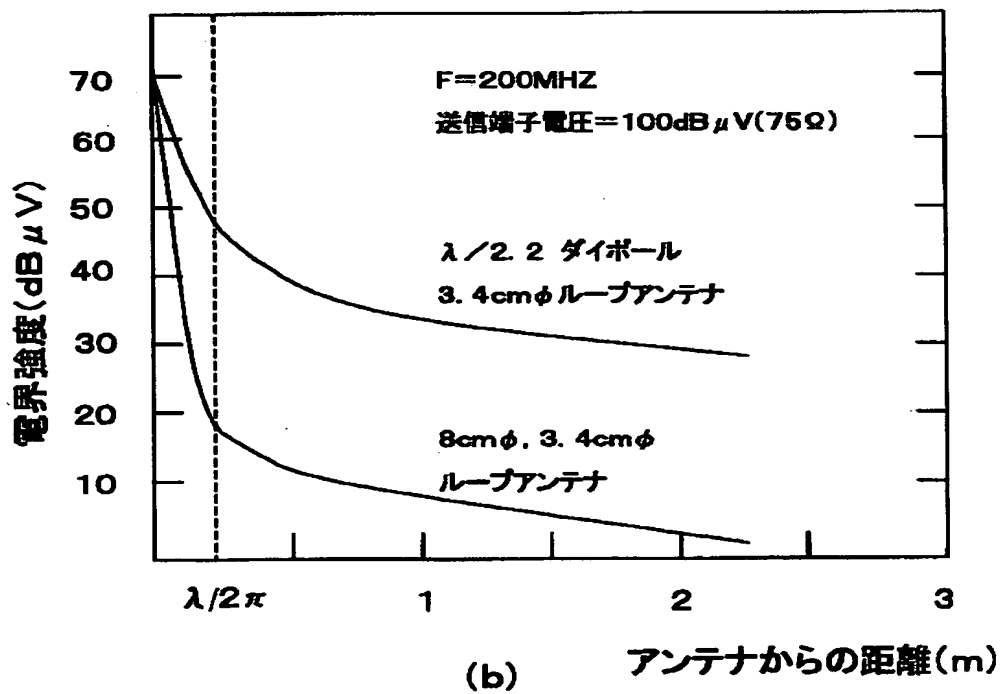
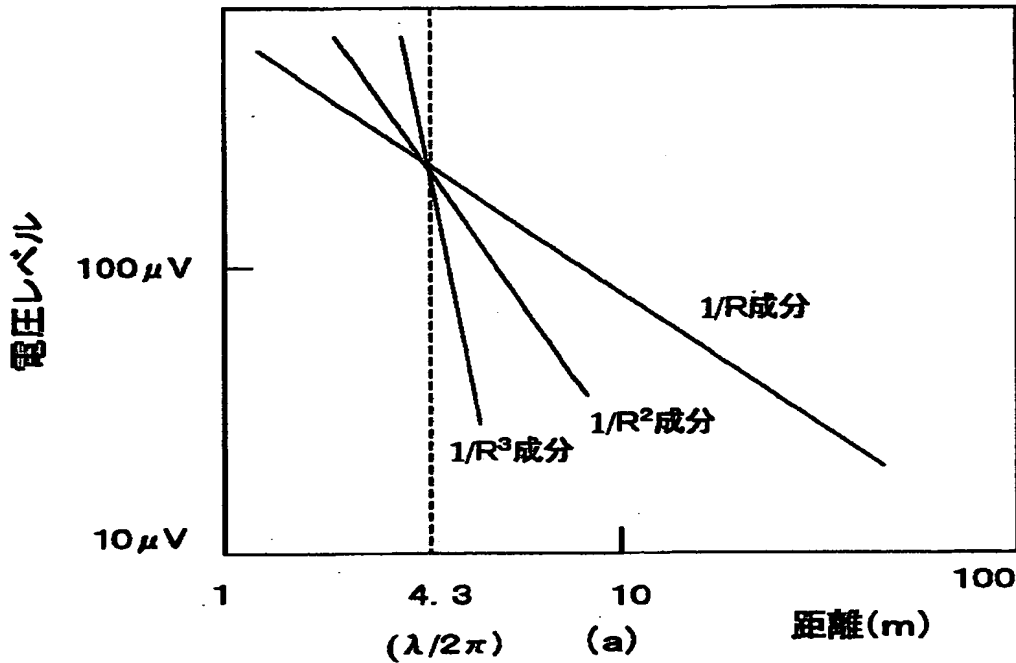
【図 1】



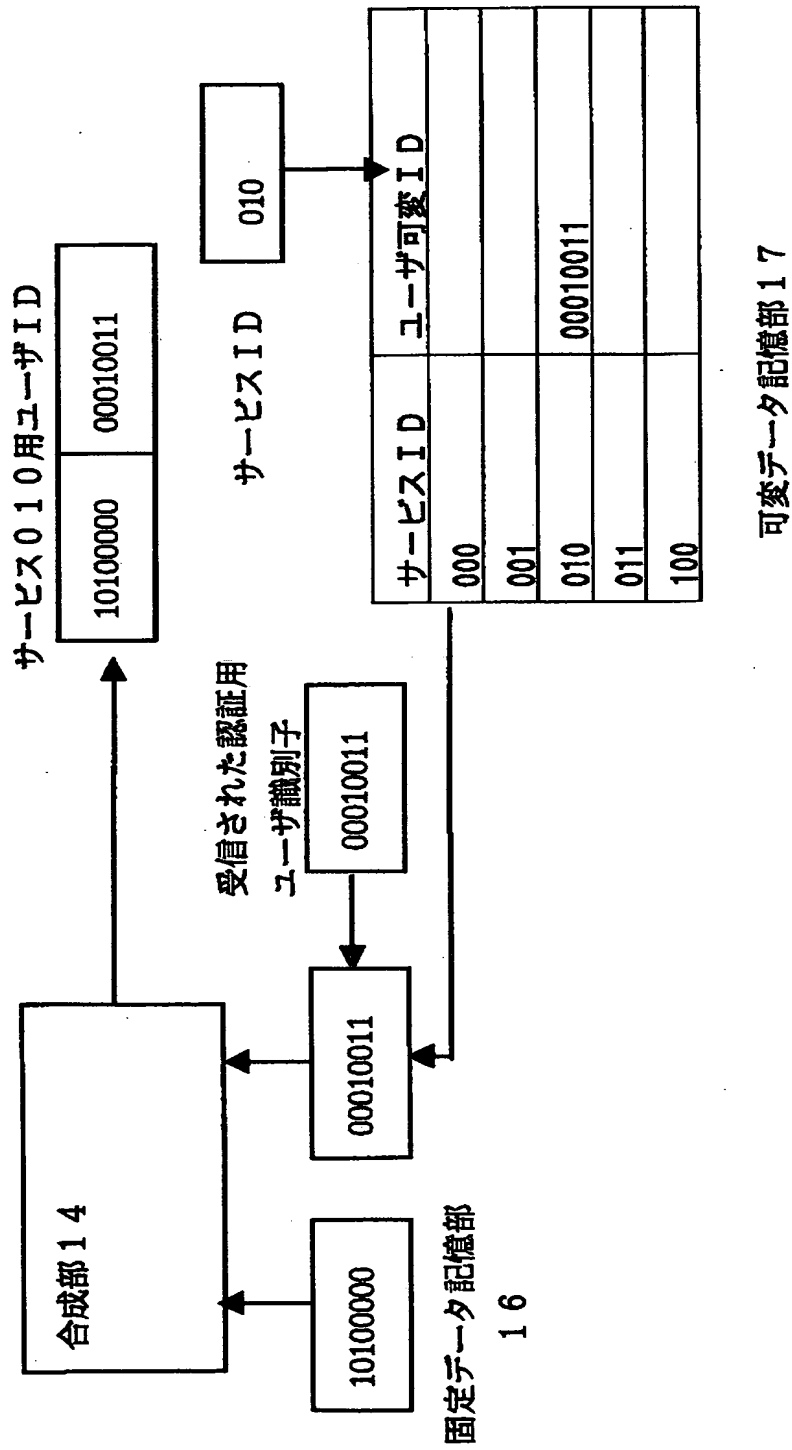
【図 2】



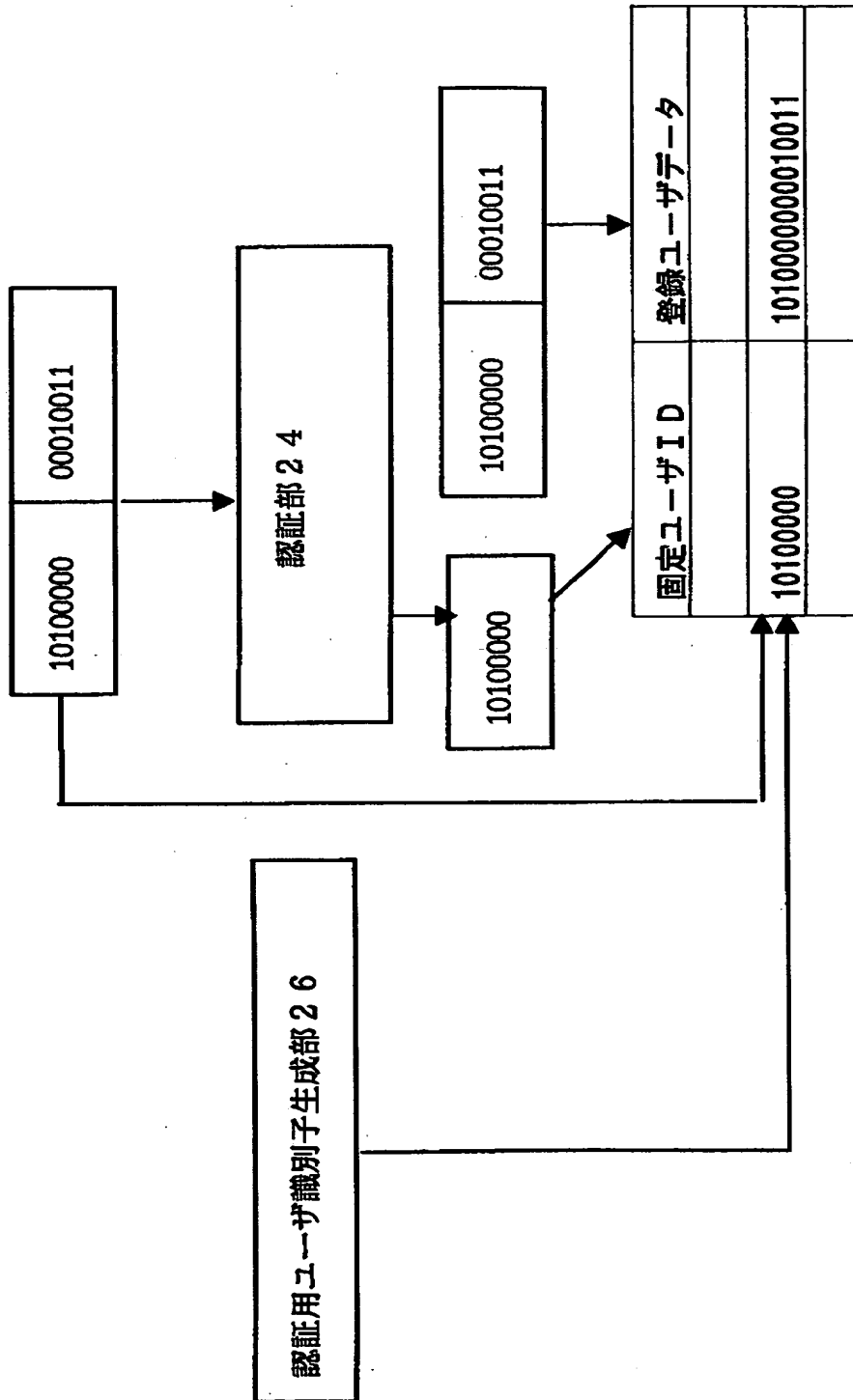
【図 3】



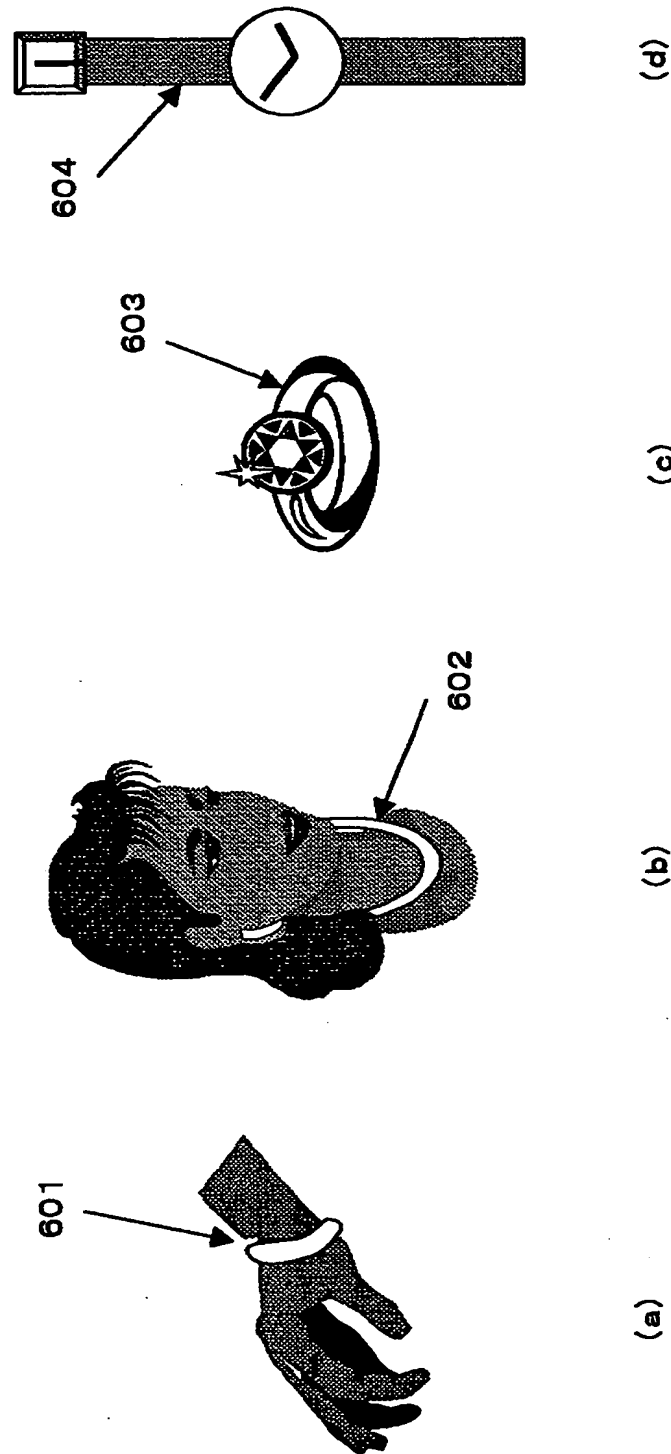
【図 4】



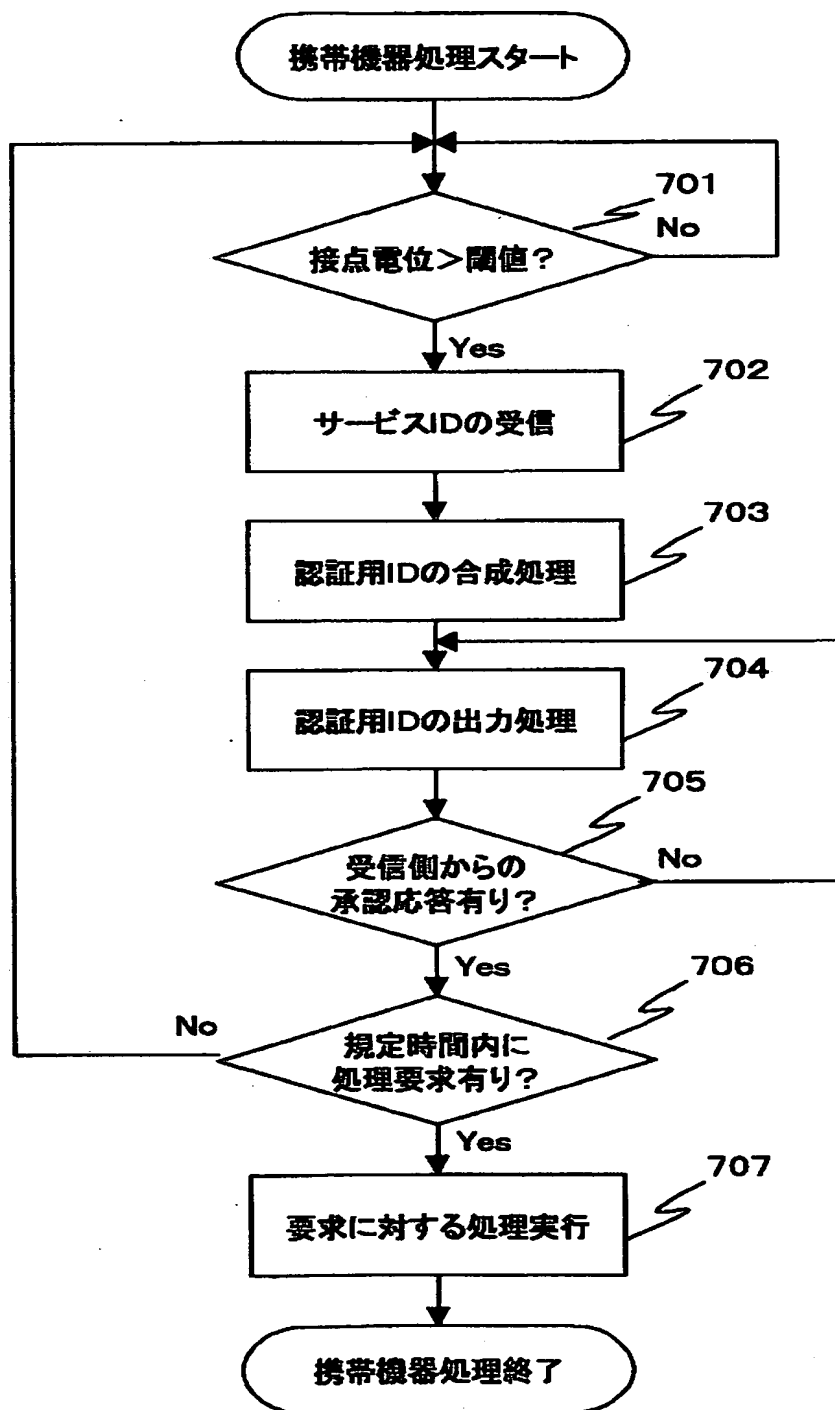
【図 5】



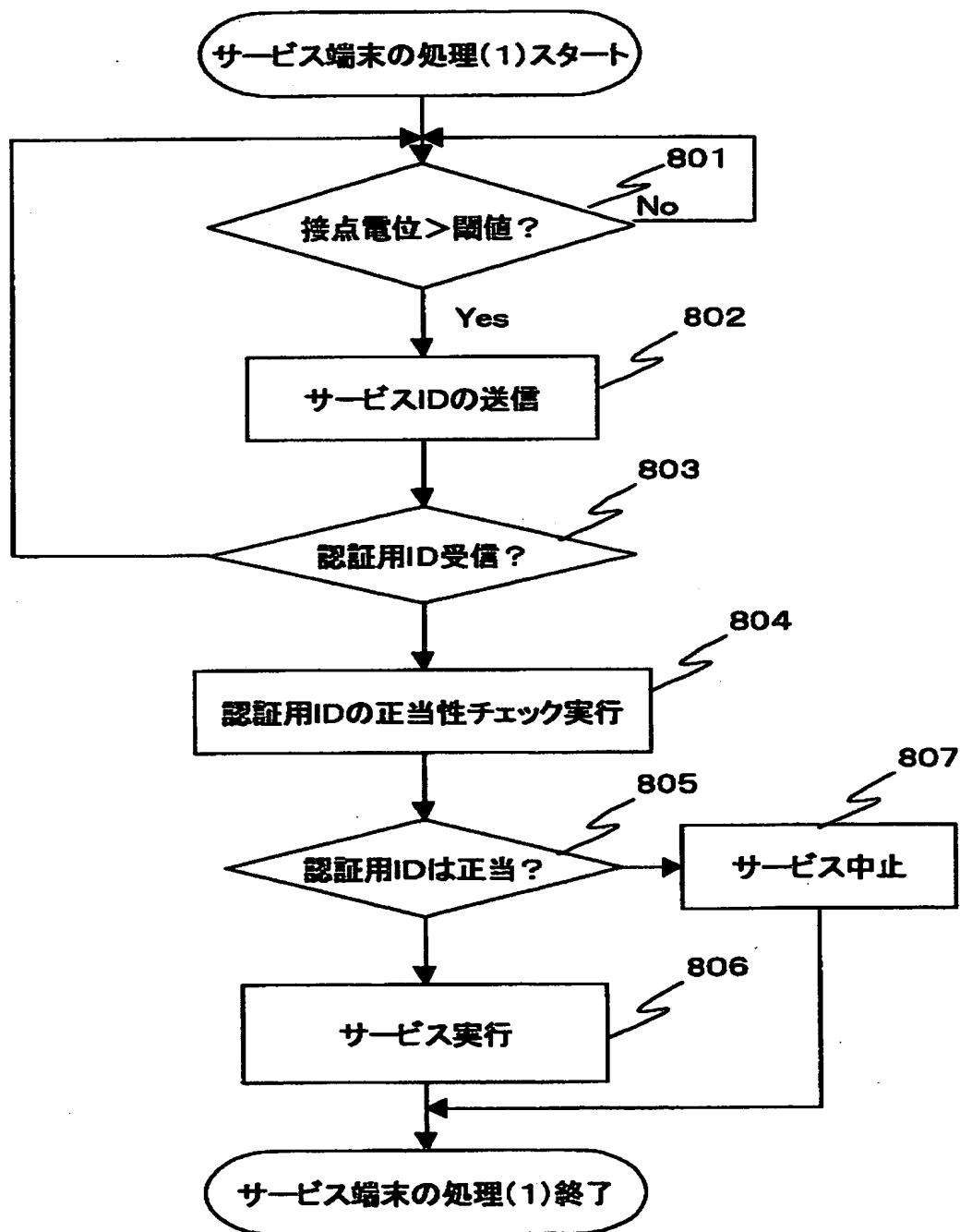
【図 6】



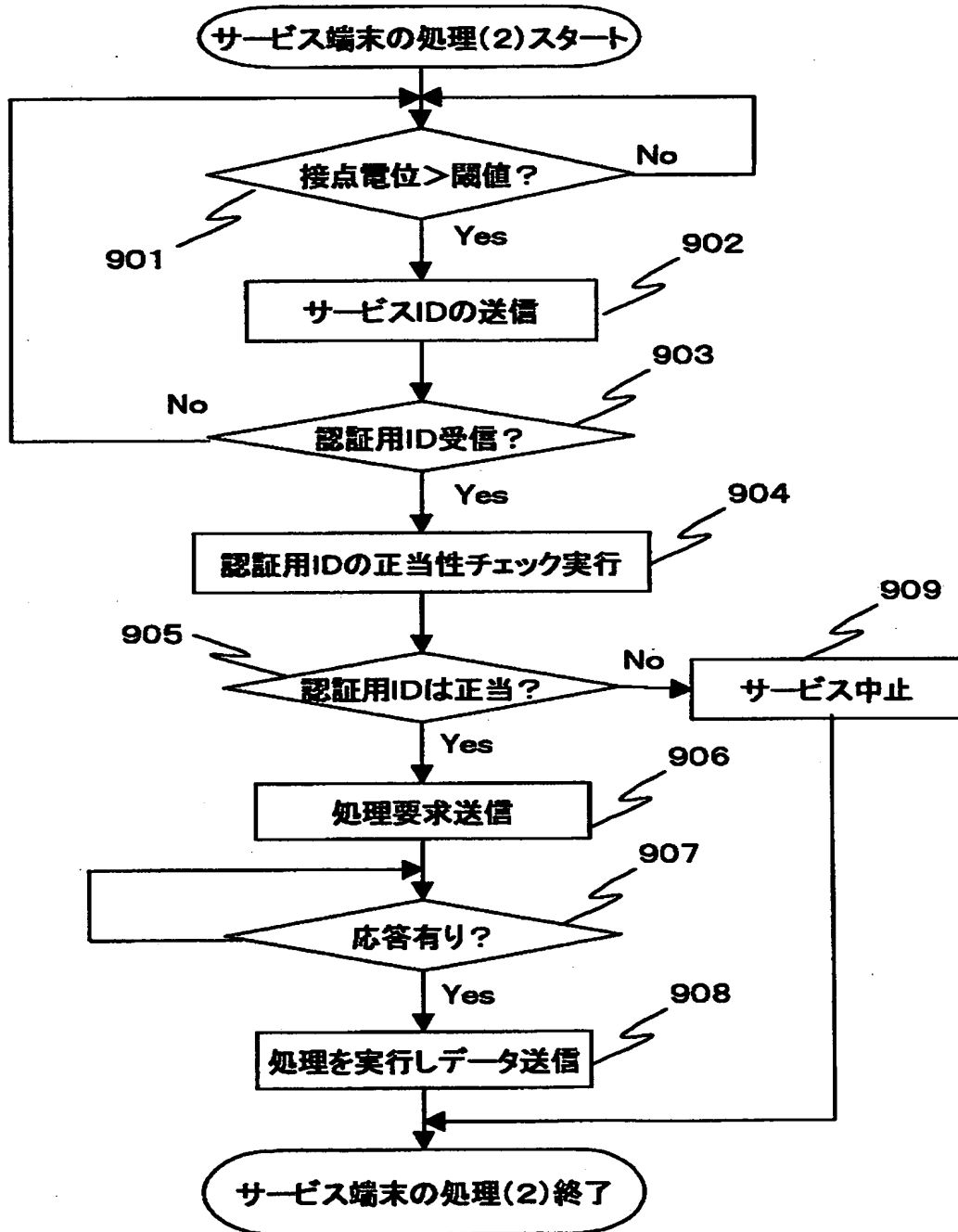
【図 7】



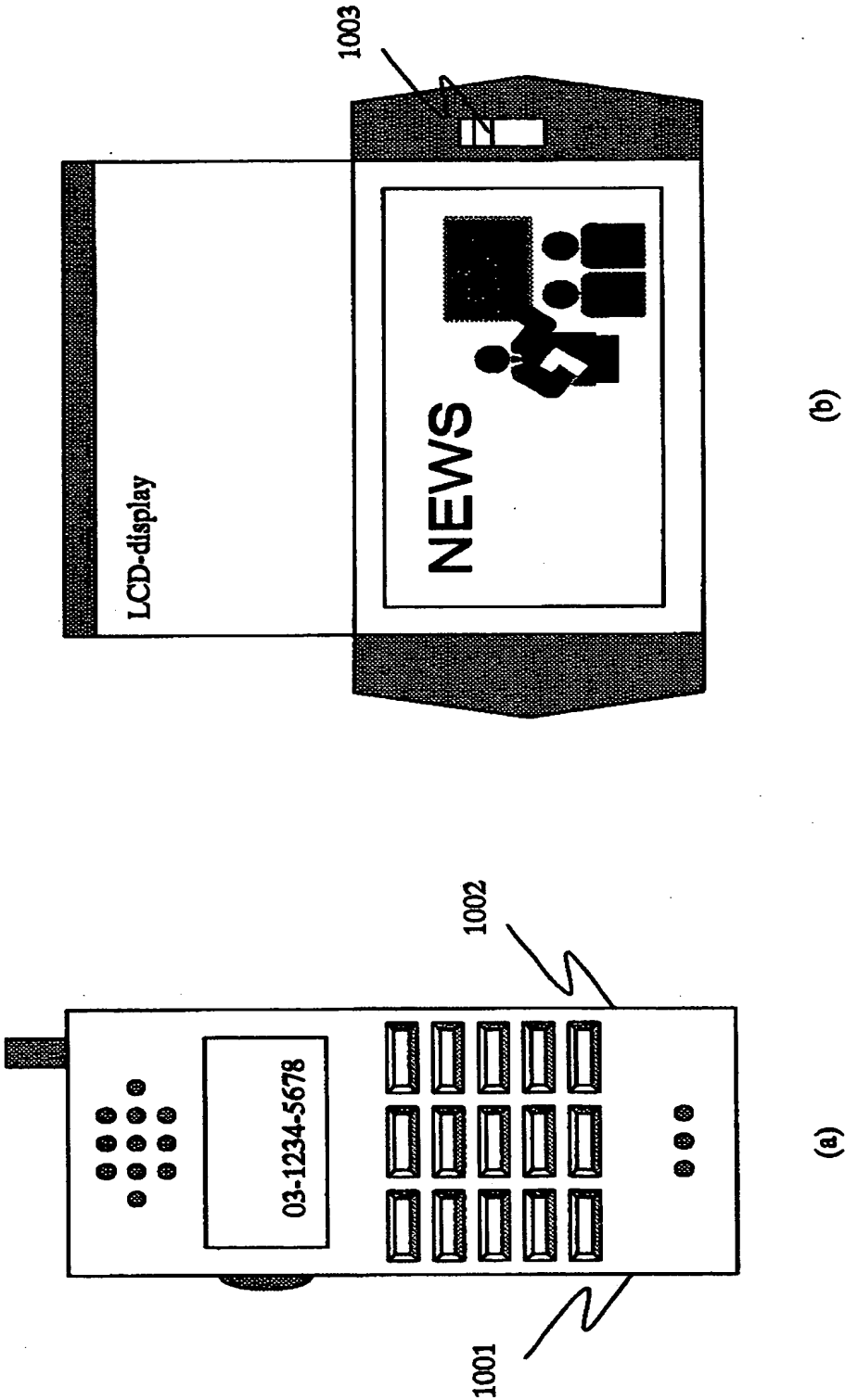
【図 8】



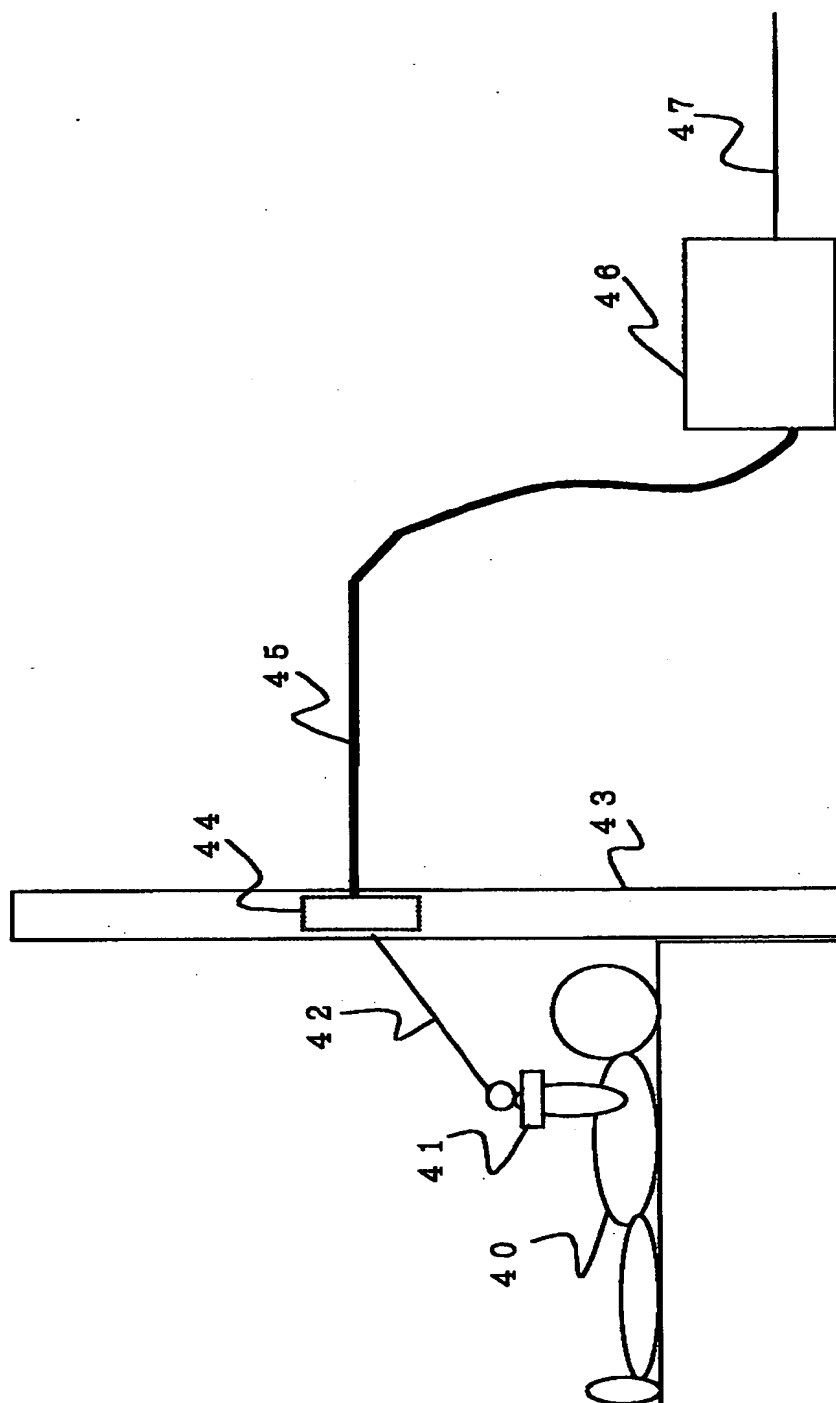
【図 9】



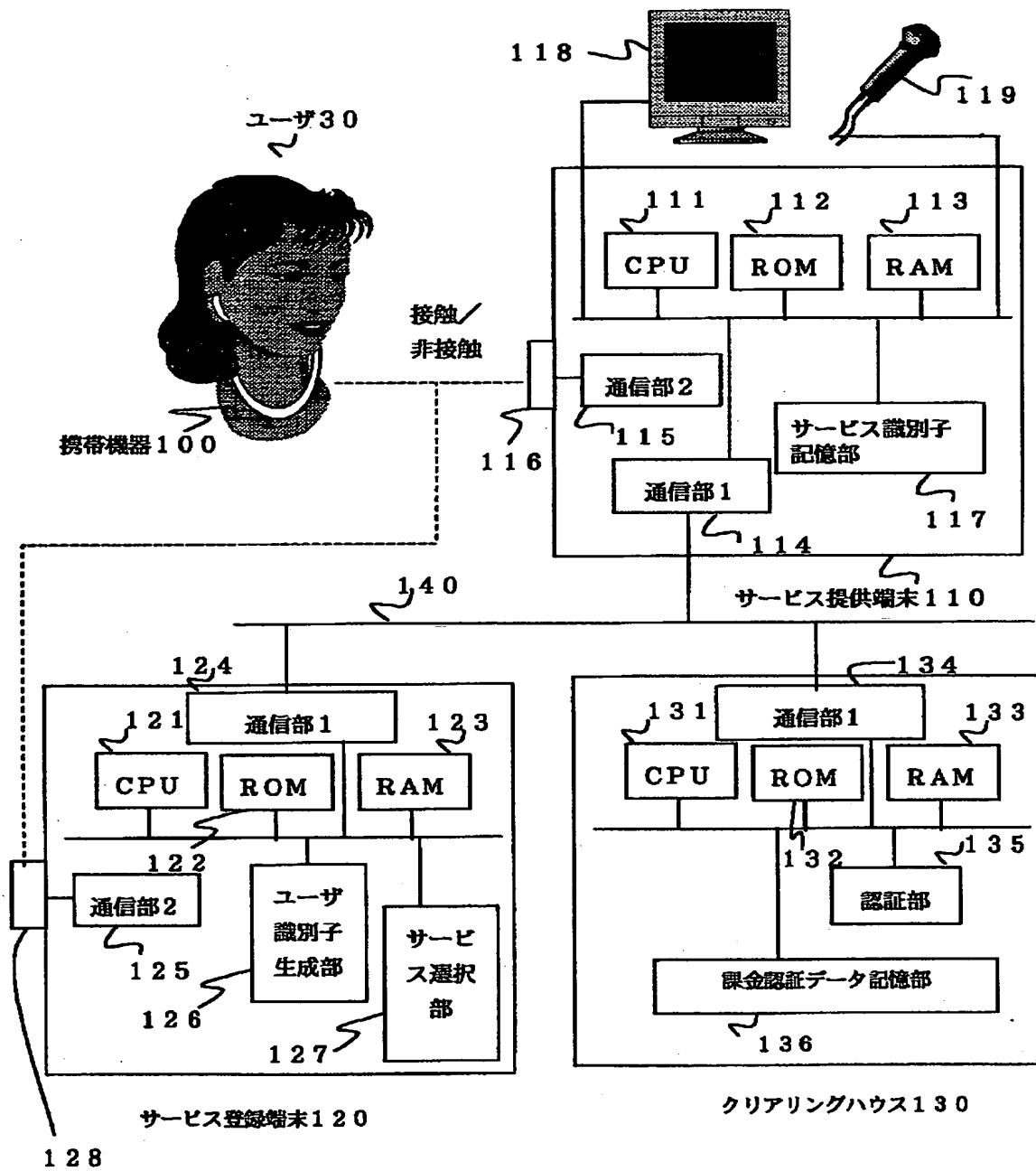
【図 1 0】



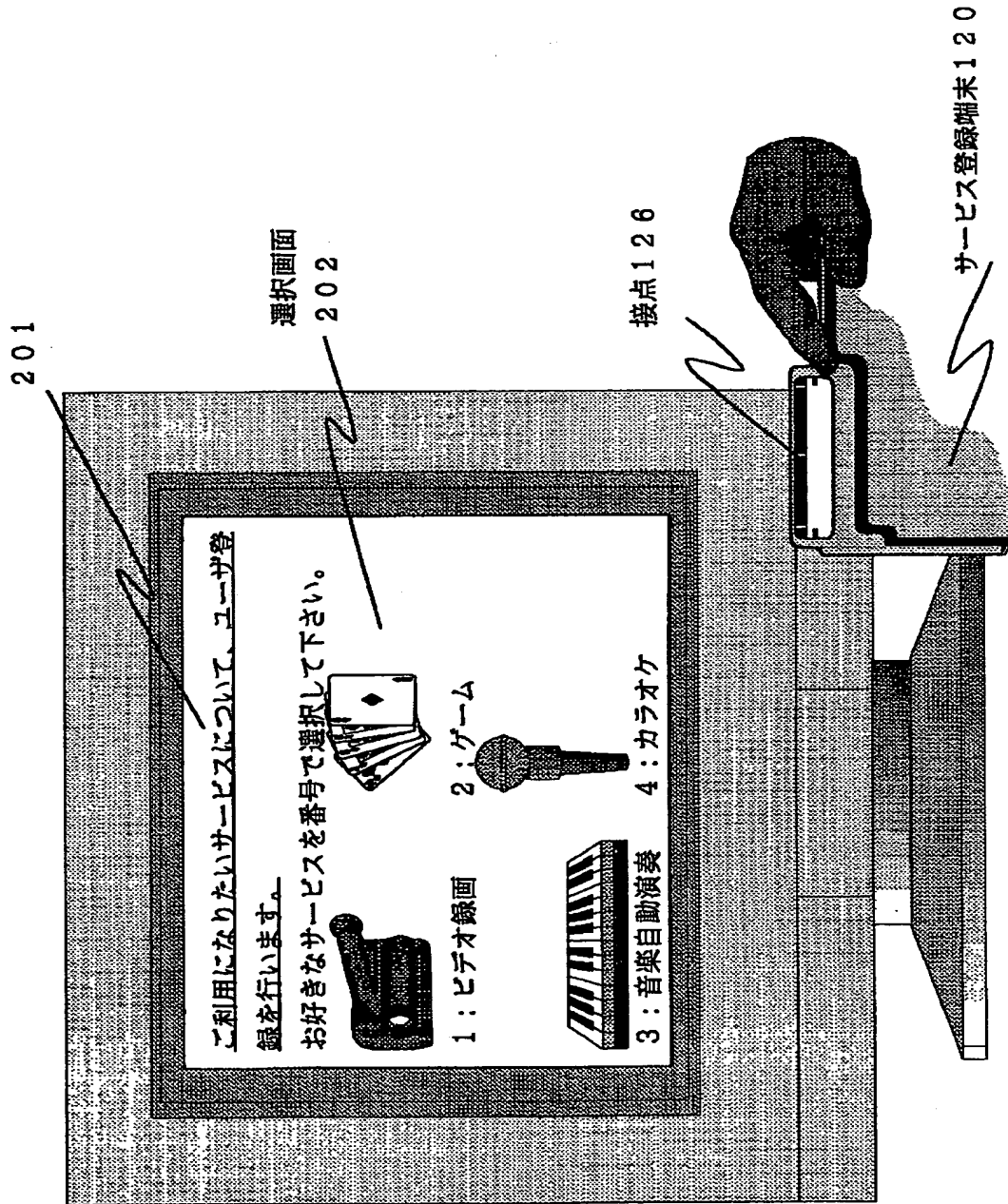
【図 11】



【図 12】



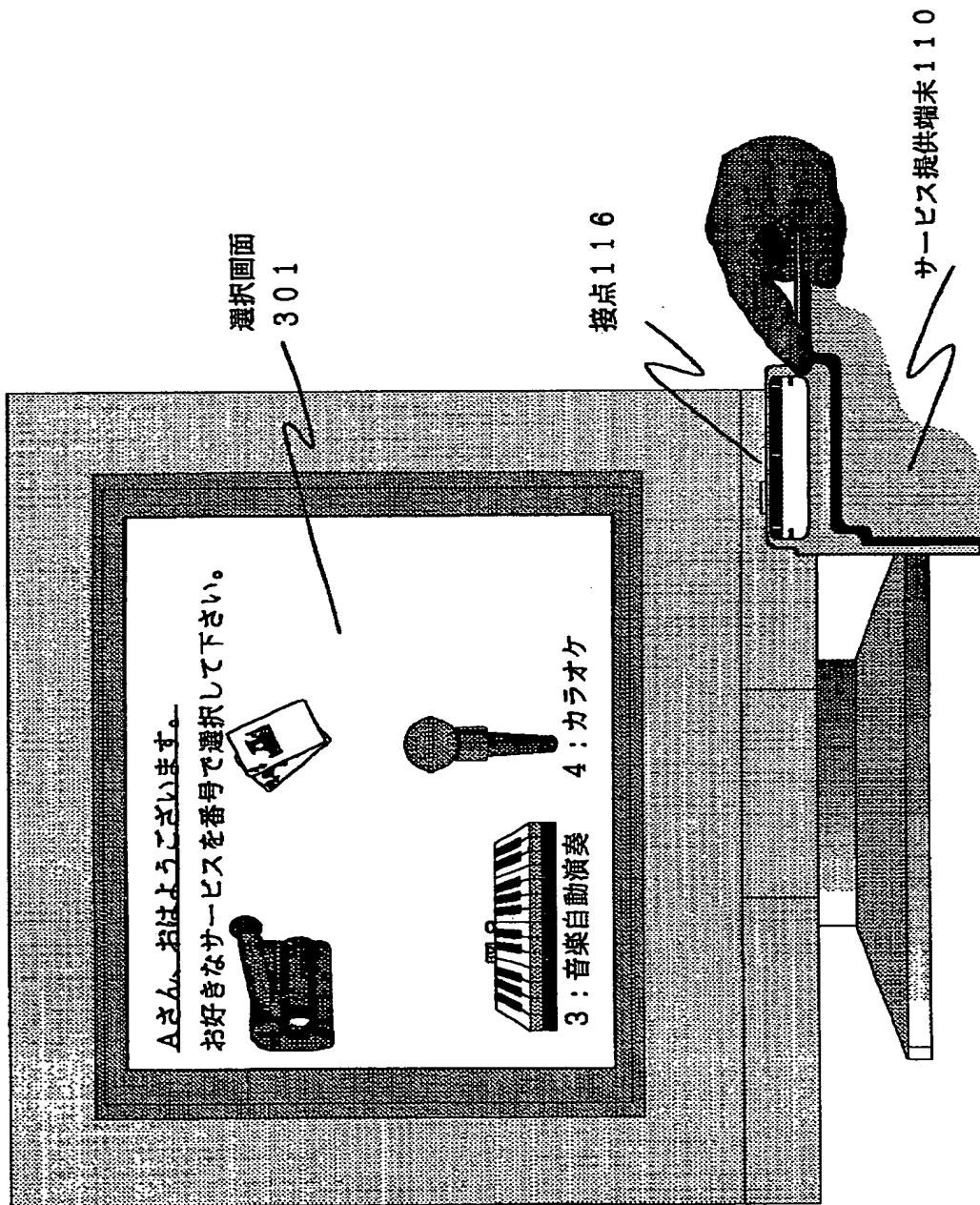
【図 13】



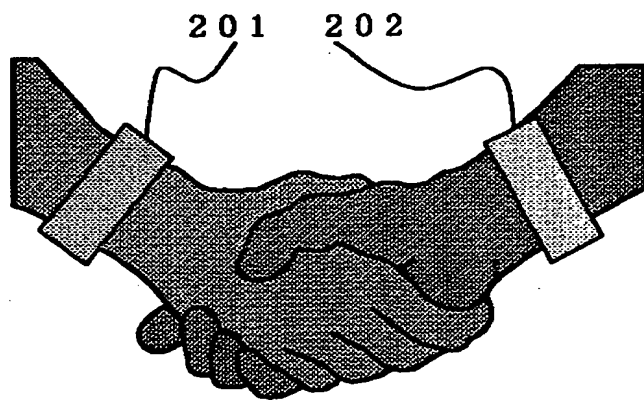
【図 1 4】

固定ユーザID	登録ユーザデータ	最大使用度数	現在使用度数
10100000	1010000000010011	100	35

【図 15】



【図 16】



【書類名】 要約書

【要約】

【課題】 人体を介した通信による個人認証処理実行システムにおいて、提供サービスに応じた認証を効率的に実行するシステムを提供する。

【解決手段】 ユーザが装着した携帯機器とサービス提供端末間での認証処理をサービス提供端末の接点に人体が触れることで実行する。ユーザの接触という物理的実感をともなって処理が行なわれる。さらに、ユーザの機器にユーザ固有識別子と、サービス端末の提供するサービスに応じて各ユーザごとに生成されるユーザ可変識別子とを格納し、サービス端末から送信されるサービス識別子に応じて、携帯端末で少なくともユーザ可変識別子に基づくサービス固有ユーザ識別データを生成してサービス端末に送付する構成とし、サービス内容に応じたユーザ単位の課金処理等、様々なユーザ管理を実行する。

【選択図】 図 1

特平 11-310517



出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社